IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Plaintiffs,

v.

ASUSTEK COMPUTER INC.,
ASUS COMPUTER INTERNATIONAL,

Defendants.

MICROSOFT CORPORATION,

Intervenor-Plaintiff,

v.

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Intervenor-Defendants.

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Intervenor-
Defendants/Counterclaim
Plaintiffs in Intervention

v.

MICROSOFT CORPORATION

Intervenor-
Plaintiff/Counterclaim
Defendant in
Intervention

AND

Case No.: 15-1125-GMS

JURY TRIAL DEMANDED

MICROSOFT MOBILE INC.

Counterclaim Defendant in Intervention

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Plaintiffs,

v.

VISUAL LAND, INC.

Defendant.

Case No.: 15-1127-GMS

JURY TRIAL DEMANDED

MICROSOFT CORPORATION,

Intervenor-Plaintiff,

v.

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Intervenor-Defendants.

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Intervenor-Defendants/Counterclaim Plaintiffs in Intervention

v.

MICROSOFT CORPORATION

Intervenor-

Plaintiff/Counterclaim Defendant in Intervention

AND

MICROSOFT MOBILE INC.

Counterclaim Defendant in Intervention

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Plaintiffs,

v.

DOUBLE POWER TECHNOLOGY, INC.,
ZOWEE MARKETING CO., LTD.,
SHENZEN ZOWEE TECHNOLOGY CO., LTD.

Defendants.

Case No.: 15-1130-GMS

JURY TRIAL DEMANDED

MICROSOFT CORPORATION,

Intervenor-Plaintiff,

v.

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Intervenor-Defendants.

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Intervenor-

Defendants/Counterclaim Plaintiffs in Intervention

v.

MICROSOFT CORPORATION

Intervenor-Plaintiff/Counterclaim Defendant in Intervention

AND

MICROSOFT MOBILE INC.

Counterclaim Defendant in Intervention

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Plaintiffs,

v.

YIFANG USA, INC. D/B/A E-FUN, INC.,

Defendant.

Case No.: 15-1131-GMS

JURY TRIAL DEMANDED

MICROSOFT CORPORATION,

Intervenor-Plaintiff,

v.

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Intervenor-Defendants.

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Intervenor-Defendants/Counterclaim Plaintiffs in Intervention

v.

MICROSOFT CORPORATION

Intervenor-Plaintiff/Counterclaim Defendant in Intervention

AND

MICROSOFT MOBILE INC.

Counterclaim Defendant in Intervention

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Plaintiffs,

v.

ACER INC.,
ACER AMERICA CORPORATION,

Defendants.

Case No.: 15-1170-GMS

JURY TRIAL DEMANDED

MICROSOFT CORPORATION,

Intervenor-Plaintiff,

v.

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Intervenor-Defendants.

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Intervenor-Defendants/Counterclaim Plaintiffs in Intervention

v.

MICROSOFT CORPORATION

Intervenor-Plaintiff/Counterclaim Defendant in Intervention

AND

MICROSOFT MOBILE INC.

Counterclaim Defendant in Intervention

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Plaintiffs,

v.

HTC CORP.,
HTC AMERICA, INC.

Defendants.

Case No.: 15-1126-GMS

JURY TRIAL DEMANDED

KONINKLIJKE PHILIPS N.V.,
U.S. PHILIPS CORPORATION,

Plaintiffs,

v.

SOUTHERN TELECOM, INC.,

Defendant.

Case No.: 15-1128-GMS

JURY TRIAL DEMANDED

JOINT APPENDIX OF INTRINSIC EVIDENCE

Tab	Description	Party Citing	Page (s)
1.	U.S. Patent No. RE 44,913 (PHILIPS00003505 to 3516)	Philips & Defendants	A-0001 to A-0012
2.	U.S. Patent Nos. 6,690,387 (PHILIPS00005195 to 5201)	Philips & Defendants	A-0013 to A-0019
3.	U.S. Patent No. 7,184,064 (PHILIPS00005844 to 5851)	Philips & Defendants	A-0020 to A-0027
4.	U.S. Patent No. 7,529,806 (PHILIPS00005961 to 5968)	Philips & Defendants	A-0028 to A-0035
5.	U.S. Patent No. 5,910,797 (PHILIPS00004054 to 4059)	Philips & Defendants	A-0036 to A-0041
6.	U.S. Patent No. 6,522,695 (PHILIPS00004779 to 4789)	Philips & Defendants	A-0042 to A-0052
7.	U.S. Patent No. 8,543,819 (PHILIPS00006372 to 6381)	Philips & Defendants	A-0053 to A-0062
8.	U.S. Patent No. 9,436,809 (PHILIPS00014257 to 14267)	Philips & Defendants	A-0063 to A-0073
9.	U.S. Patent No. 6,772,114 (PHILIPS00005268 to 5275)	Philips & Defendants	A-0074 to A-0081
10.	U.S. Patent No. RE43,564 (PHILIPS00002694 to 2700)	Philips & Defendants	A-0082 to A-0088
11.	U.S. Patent No. 6,211,856 (PHILIPS00014247 to 14256)	Philips	A-0089 to A-0098

12.	’913 Patent file history, 10/06/2004 Allowance (PHILIPS00005829 to 5833)	Philips	A-0099 to A-0103
13.	’806 Patent file history, 10/01/2002 Amendment (PHILIPS00006092 to 6101)	Philips	A-0104 to A-0113
14.	’806 Patent file history, 09/08/2003 Appeal (PHILIPS00006131 to 6136)	Philips & Defendants	A-0114 to A-0119
15.	’806 Patent file history, 02/19/2004 Remarks (PHILIPS00006154 to 6157)	Philips & Defendants	A-0120 to A-0123
16.	’806 Patent file history, 07/27/2004 Appeal (PHILIPS00006170 to 6175)	Defendants	A-0124 to A-0129
17.	’806 Patent file history, 10/05/2004 Rejection (PHILIPS00006184 to 6193)	Philips	A-0130 to A-0139
18.	’806 Patent file history, 09/01/2005 Appeal (PHILIPS00006218 to 6226)	Philips & Defendants	A-0140 to A-0148
19.	’806 Patent file history, 08/18/2006 Appeal (PHILIPS00006260 to 6268)	Defendants	A-0149 to A-0157
20.	’806 Patent file history, 06/24/2008 Rejection (PHILIPS00006305 to 6313)	Philips	A-0158 to A-0166
21.	’806 Patent file history, 09/23/2008 Amendment (PHILIPS00006315 to 6326)	Defendants	A-0167 to A-0178
22.	’797 Patent file history, 5/22/1998 Amendment (PHILIPS00004212 to 4217) Also referred to as: ’797 Patent file history, 5/22/1997 Amendment	Philips & Defendants	A-0179 to A-0184
23.	’797 Patent file history, 10/26/1998 Amendment (PHILIPS00004229 to 4233)	Defendants	A-0185 to A-0189

24.	’797 Patent file history, 01/12/1999 Notice of Allowability (PHILIPS00004234 to 4235)	Philips	A-0190 to A-0191
25.	’797 Patent file history, 05/05/1999 Response (PHILIPS00004245 to 4246)	Philips	A-0192 to A-0193
26.	’819 Patent file history, 10/28/2010 Rejection (PHILIPS00006439 to 6453)	Defendants	A-0194 to A-0208
27.	’819 Patent file history, 02/17/2011 Rejection (PHILIPS00006480 to 6501)	Defendants	A-0209 to A-0230
28.	’819 Patent file history, 07/18/2011 Response (PHILIPS00006537 to 6549)	Philips	A-0231 to A-0243
29.	’819 Patent file history, 12/14/2011 Amendment (PHILIPS00006579 to 6591)	Philips	A-0244 to A-0256
30.	’819 Patent file history, 01/05/2012 Rejection (PHILIPS00006595 to 6617)	Philips & Defendants	A-0257 to A-0279
31.	’819 Patent file history, 06/01/2012 RCE (PHILIPS00006719 to 6732)	Philips & Defendants	A-0280 to A-0293
32.	’819 Patent file history, 08/31/2012 Rejection (PHILIPS00006981 to 7008)	Philips	A-0294 to A-0321
33.	’819 Patent file history, 01/04/2013 Rejection (PHILIPS00007047 to 7079)	Defendants	A-0322 to A-0354
34.	’819 Patent file history, 03/01/2013 Amendment (PHILIPS00007083 to 7104)	Philips	A-0355 to A-0376
35.	’819 Patent file history, 03/11/2013 Advisory (PHILIPS00007108 to 7110)	Philips	A-0377 to A-0379

36.	ISO/IEC 9798 International Standard (Section 1, dated 8/1/1997; Section 2, dated 7/15/1999; Section 3, dated 10/15/1999; Section 4, dated 12/15/1999; Section 5, dated 3/15/1999)[*] (PHILIPS00014075 to 14159)	Philips	A-0380 to A-0464
37.	ISO/IEC 11770 International Standard (Section 1, dated 12/15/1996; Section 2, dated 4/15/1996; Section 3, dated 11/1/1999)[1] (PHILIPS00014160 to 14246)	Philips & Defendants	A-0465 to A-0551
38.	'114 Patent file history, 9/21/2003 Rejection (PHILIPS00005560 to 5569)	Defendants	A-0552 to A-0561
39.	'114 Patent file history, 11/20/2003 Remarks (PHILIPS00005570 to 5583)	Philips & Defendants	A-0562 to A-0575
40.	'203 Patent file history, 5/30/2002 Notice of Allowability (PHILIPS00004654 to 4659)	Philips & Defendants	A-0576 to A-0581

[1] For the reasons stated in Defendants' Answering Claim Construction Brief, Defendants contend that ISO/IEC 9798 and ISO/IEC 11770 are not intrinsic evidence and should not be included in this Appendix.

MCCARTER & ENGLISH, LLP

/s/ Daniel M. Silver
Michael P. Kelly (#2295)
Daniel M. Silver (#4758)
Benjamin A. Smyth (#5528)
Renaissance Centre
405 N. King Street, 8th Floor
Wilmington, DE 19801
(302) 984-6300
mkelly@mccarter.com
dsilver@mccarter.com
bsmyth@mccarter.com

Michael P. Sandonato
John D. Carlin
Daniel A. Apgar
Jonathan M. Sharret
FITZPATRICK, CELLA, HARPER & SCINTO
1290 Avenue of the Americas
New York, NY 10104-3800
(212) 218-2100

Attorneys for Plaintiffs

DATED: April 7, 2017

MORRIS, NICHOLS, ARSHT & TUNNELL LLP

/s/ Rodger D. Smith II
Rodger D. Smith II (#3778)
Eleanor G. Tennyson (#5812)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
rsmith@mnat.com
etennyson@mnat.com

Matt Warren
Patrick Shields
Brian Wikner
Erika Mayo
WARREN LEX LLP
2261 Market Street, No. 606
San Francisco, CA 94114

Attorneys for Defendants Acer, Inc., Acer America Corporation, ASUSTeK Computer Inc. and ASUS Computer International

Kai Tseng
Craig Kaufman
James Lin
TECHKNOWLEDGE LAW GROUP LLP
100 Marine Parkway, Suite 200
Redwood Shores, CA 94065

Attorneys for Defendants Acer, Inc., Acer America Corporation

Michael J. Newton
Derek Neilson
Sang (Michael) Lee
ALSTON & BIRD LLP
2828 N. Harwood Street, Suite 1800
Dallas, TX 75201-2139

Patrick J. Flinn
ALSTON & BIRD LLP
1201 West Peachtree Street, Suite 4900
Atlanta, GA 30309-3424

YOUNG CONAWAY STARGATT
& TAYLOR, LLP

/s/ Adam W. Poff
Adam W. Poff (#3990)
Anne Shea Gaza (#4093)
Samantha G. Wilson (#5816)
Rodney Square
1000 North King Street
Wilmington, DE 19801
(302) 571-6600
apoff@ycst.com
agaza@ycst.com
swilson@ycst.com

Attorneys for Defendant Visual Land, Inc.

Xavier M. Brandwajn
ALSTON & BIRD LLP
1950 University Avenue, 5th Floor
East Palo Alto, CA 94303

Ross R. Barton
ALSTON & BIRD LLP
101 South Tyron Street, Suite 4000
Charlotte, NC 28280-4000
(704) 444-1000

Attorneys for Defendants ASUSTeK Computer Inc. and ASUS Computer International

YOUNG CONAWAY STARGATT
& TAYLOR, LLP

/s/ Karen L. Pascale
Karen L. Pascale (#2903)
Robert M. Vrana (# 5666)
Rodney Square
1000 North King Street
Wilmington, DE 19801
(302) 571-6600
apoff@ycst.com
agaza@ycst.com
swilson@ycst.com

P. Andrew Blatt
WOOD HERRON & EVANS LLP
2700 Carew Tower
Cincinnati, OH 45202
(513) 241-2324

Attorneys for Defendant Southern Telecom, Inc.

SHAW KELLER LLP

/s/ Karen E. Keller
John W. Shaw (# 3362)
Karen E. Keller (# 4489)
Andrew E. Russell (# 5382)
300 Delaware Avenue, Suite 1120
Wilmington, DE 19801
(302) 298-0700
jshaw@shawkeller.com
kkeller@shawkeller.com
arussell@shawkeller.com

John Schnurer
Kevin Patariu
Ryan Hawkins
Louise Lu
Vinay Sathe
PERKINS COIE LLP
11988 El Camino Real, Suite 350
San Diego, CA 92130
(858) 720-5700

Ryan McBrayer
Jonathan Putman
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
(206) 359-8000

Attorneys for Defendants HTC Corp. and HTC America, Inc.

SHAW KELLER LLP

/s/ Karen E. Keller
John W. Shaw (# 3362)
Karen E. Keller (# 4489)
Andrew E. Russell (# 5382)
300 Delaware Avenue, Suite 1120
Wilmington, DE 19801
(302) 298-0700
jshaw@shawkeller.com
kkeller@shawkeller.com
arussell@shawkeller.com

Lucian C. Chen
Wing K. Chiu
LUCIAN C. CHEN, ESQ. PLLC
One Grand Central Place
60 East 42nd Street, Suite 4600
New York, NY 10165
(212) 710-3007

Attorneys for Defendant YiFang USA, Inc. D/B/A E-Fun, Inc.

MORRIS, NICHOLS, ARSHT
& TUNNELL LLP

/s/ Karen Jacobs
Karen Jacobs (#2881)
Mirco J. Haag (#6165)
1201 North Market Street
P.O. Box 1347
Wilmington, DE 19899
(302) 658-9200
kjacobs@mnat.com
mhaag@mnat.com

Bryan G. Harrison
LOCKE LORD LLP
Terminus 200
3333 Piedmont Road NE, Suite 1200
Atlanta, GA 30305
(404) 870-4629

Attorneys for Defendants
Double Power Technology, Inc.,
Zowee Marketing Co., Ltd. and
Shenzen Zowee Technology Co., Ltd.

ASHBY & GEDDES

/s/ Andrew C. Mayo
Steven J. Balick (#2114)
Andrews C. Mayo (#5207)
500 Delaware Avenue, 8th Flr.
P.O. Box 1150
Wilmington, DE 19899
(302) 654-1888
sbalick@ashby-geddes.com
amayo@ashby-geddes.com

Chad S. Campbell
Jared W. Crop
PERKINS COIE LLP
2901 N. Central Avenue, Suite 2000
Phoenix, AZ 85012-2788
(602) 351-8000

Judith Jennison
Christina McCullough
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
(206) 359-8000

Attorneys for Microsoft Corporation and Microsoft Mobile Inc.

1

US00RE44913E

(19) **United States**
(12) **Reissued Patent**
Bickerton

(10) **Patent Number: US RE44,913 E**
(45) **Date of Reissued Patent: May 27, 2014**

(54) **TEXT ENTRY METHOD AND DEVICE THEREFOR**

(71) Applicant: **Matthew J. Bickerton**, Bletchingley (GB)

(72) Inventor: **Matthew J. Bickerton**, Bletchingley (GB)

(73) Assignee: **Koninklijke Philips N.V.**, Eindhoven (NL)

(21) Appl. No.: **13/955,345**

(22) Filed: **Jul. 31, 2013**

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **6,885,318**
Issued: **Apr. 26, 2005**
Appl. No.: **10/156,409**
Filed: **May 28, 2002**

(30) **Foreign Application Priority Data**

Jun. 30, 2001 (GB) 0116083.7

(51) **Int. Cl.**
H03K 17/94 (2006.01)
G06F 15/02 (2006.01)

(52) **U.S. Cl.**
USPC **341/22**; 345/168; 708/145; 708/146; 379/368; 400/486

(58) **Field of Classification Search**
CPC H03K 17/94; G06F 15/02; G06F 3/0238
USPC 341/20, 22; 345/168; 379/368; 400/486; 708/131, 145, 146
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,967,273	A		6/1976	Knowlton	
4,099,246	A	*	7/1978	Osborne et al.	708/146
4,737,980	A		4/1988	Curtin et al.	
4,999,795	A		3/1991	Lapeyre	
5,124,940	A		6/1992	Lapeyre	
5,128,672	A		7/1992	Kaehler	
5,798,716	A		8/1998	Davis	
5,818,437	A		10/1998	Grover et al.	
5,861,823	A		1/1999	Strauch et al.	

(Continued)

FOREIGN PATENT DOCUMENTS

EP	0889388 A1	7/1999
JP	4127310	4/1992

(Continued)

OTHER PUBLICATIONS

TLS2200 Thermal Transfer Printer User's Guide, 2000 Brady Worldwide, Inc. 93 pages.

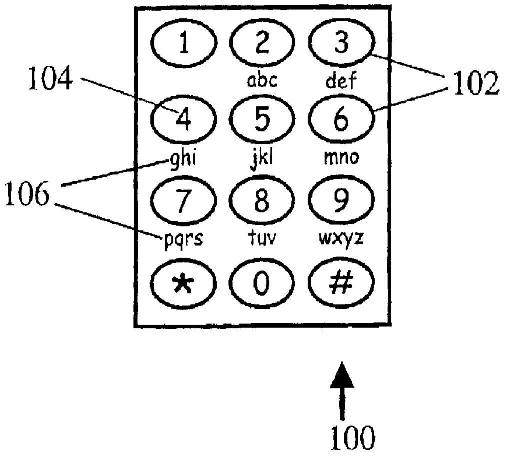
(Continued)

Primary Examiner — Albert Wong

(57) **ABSTRACT**

A method and device for improved character input are described, wherein the method employs a keypad **100** comprising keys **102** able to display secondary characters **106** in addition to primary characters **104**. The keypad has a default display state. A first key selection causes the keypad **100** to display secondary characters **106** associated with the first key on other keys **102**, whereupon a second key selection causes the displayed character to be input, following which the keypad reverts to displaying the default state. Further secondary characters **200** may also be displayed after a first key selection. The method is particularly useful for handheld devices such as mobile radio telephones or handheld computers adapted to implement the method of the invention.

16 Claims, 6 Drawing Sheets



(56) References Cited

U.S. PATENT DOCUMENTS

5,952,942	A	*	9/1999	Balakrishnan et al.	.... 341/20
5,952,952	A		9/1999	Choi et al.	
5,956,021	A		9/1999	Kubota et al.	
6,009,444	A		12/1999	Chen	
6,016,142	A		1/2000	Chang et al.	
6,016,538	A		1/2000	Guttag et al.	
6,043,760	A		3/2000	Laakkonen	
6,130,628	A		10/2000	Schneider-Hufschmidt et al.	
6,169,538	B1		1/2001	Nowlan et al.	
6,271,835	B1		8/2001	Hoeksma	
6,295,052	B1		9/2001	Kato et al.	
6,359,572	B1		3/2002	Vale	
6,473,006	B1		10/2002	Yu et al.	
6,686,902	B2		2/2004	Lee	

FOREIGN PATENT DOCUMENTS

JP	07200120	A	8/1995	
JP	0934891	A	2/1997	
JP	2000172417	A	6/2000	
JP	2001125720	A	5/2001	
JP	4019512	A	10/2007	
JP	04999794	B2	8/2012	
WO	200214996	A1	2/2002	
WO	WO 0214996		2/2002	.... G06F 3/00

OTHER PUBLICATIONS

Masui, "An Efficient Text Input Method for Pen-Based Computers", Proceedings of the ACM Conference on Human Factors in Computing System, Apr. 1998, p. 328-335.

Patent Abstracts of Japan, Ono Katsuyasu: "Adjacent Character Display Keyboard," Publication No. 07200120, Apr. 8, 1995, Application No. 05355185, Dec. 28, 1993.

* cited by examiner

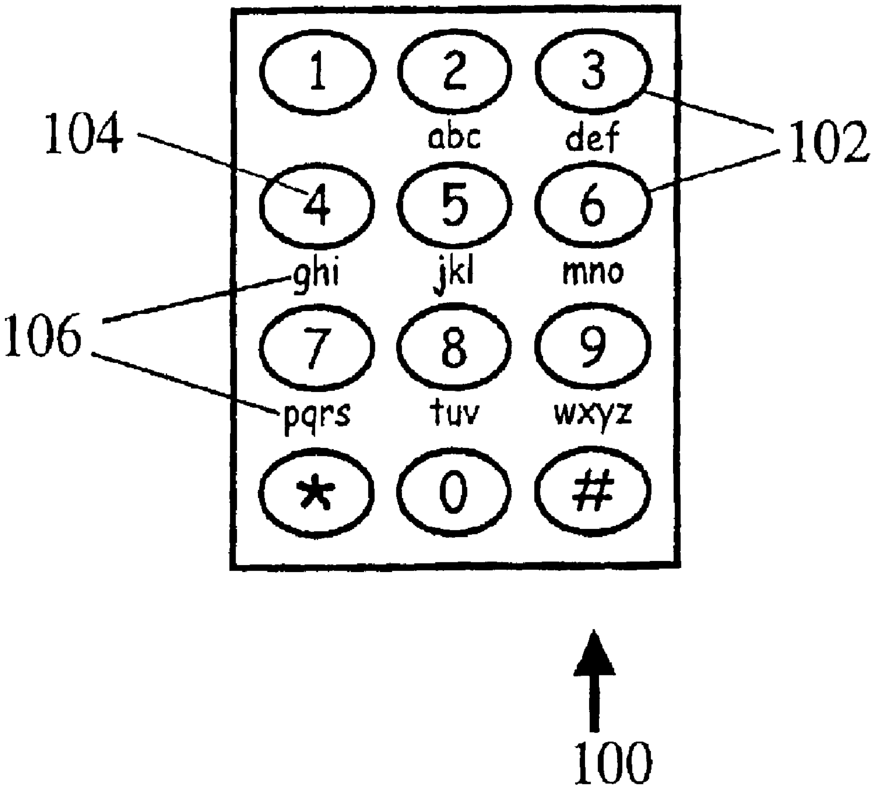


Fig. 1

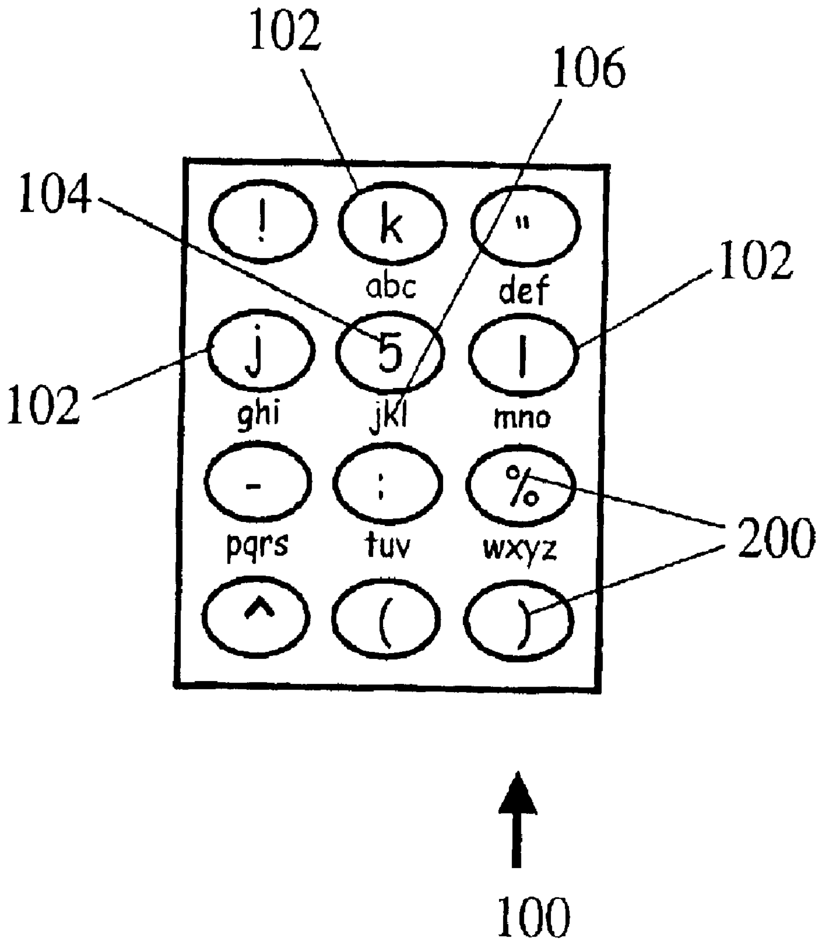

102
106
104
102
102
!
k
"
abc
def
j
5
l
ghi
jkl
mno
-
:
%
200
pqrs
tuv
wxyz
^
(
)
100

Fig. 2

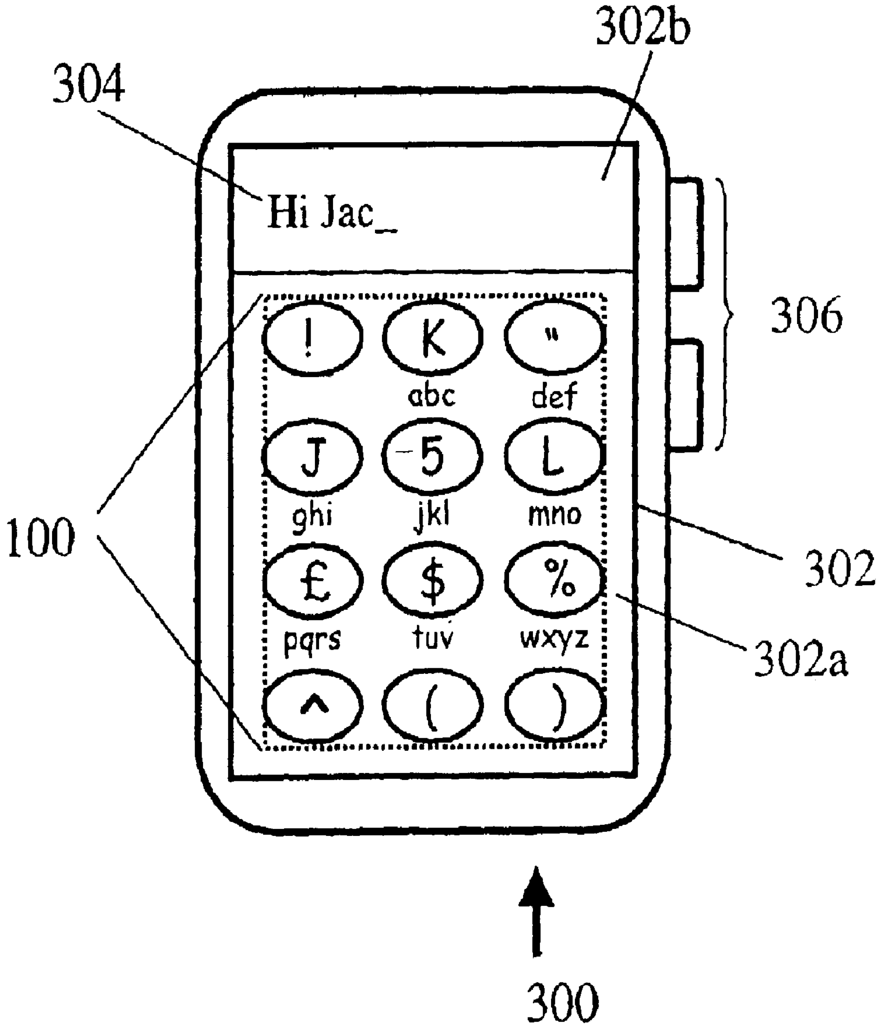

302b
304
Hi Jac_
!
K
"
abc
def
J
5
L
ghi
jkl
mno
£
$
%
pqrs
tuv
wxyz
^
(
)
306
100
302
302a
300

Fig. 3

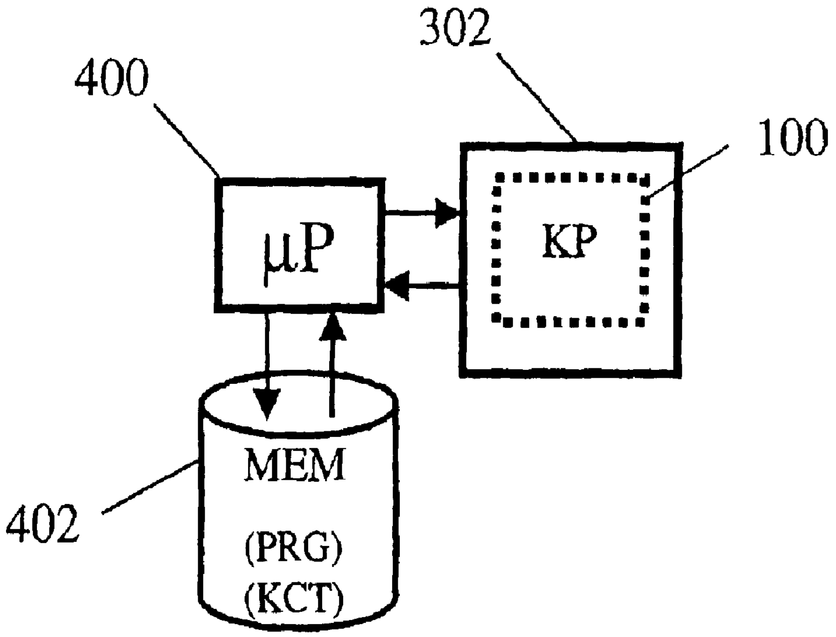


Fig. 4

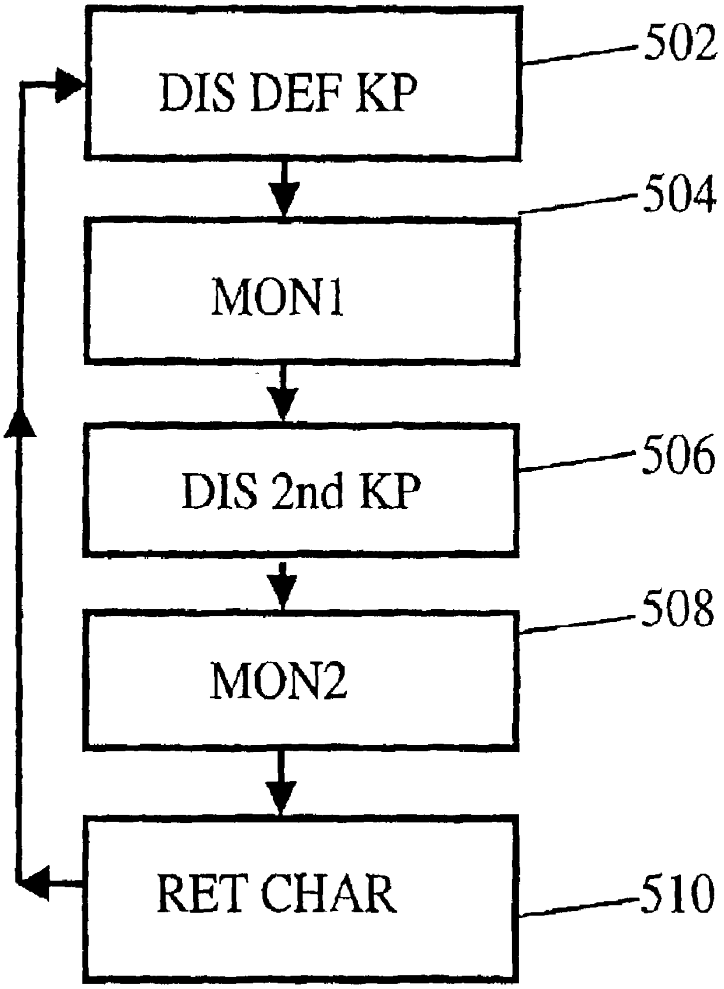


Fig. 5

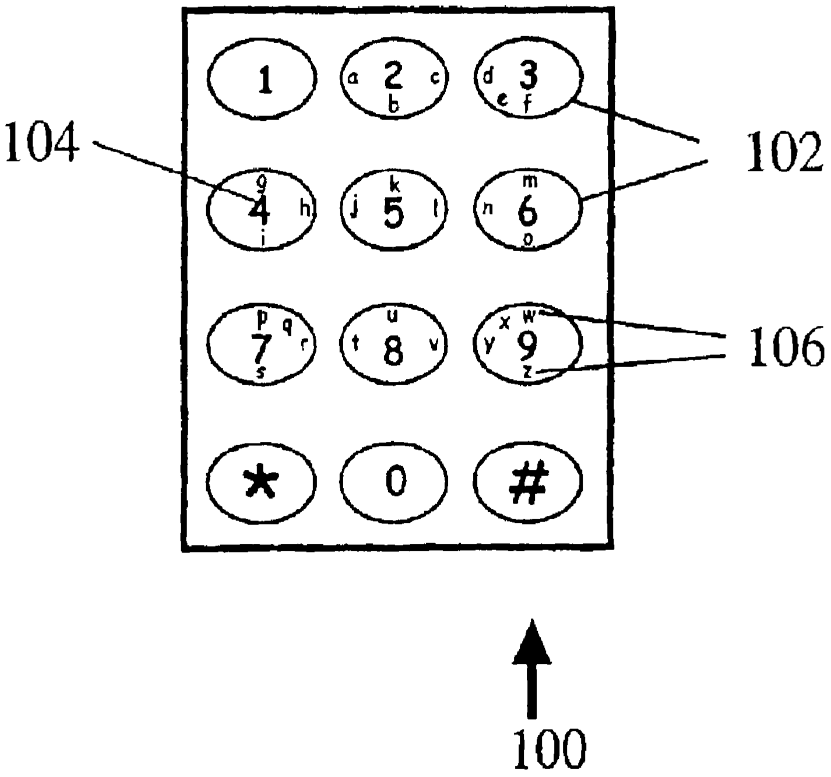


Fig. 6

TEXT ENTRY METHOD AND DEVICE THEREFOR

Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.

This application claims the benefit or priority of and describes the relationships between the following applications: wherein this application is a reissue of U.S. Pat. No. 6,885,318, issued Apr. 26, 2005, from U.S. patent application Ser. No. 10/156,409, filed May 28, 2002, which claims priority of foreign application GB 0116083.7 filed Jun. 30, 2001, all of which are incorporated herein in whole by reference.

The present invention relates to a method of entering text into a device, and to a device such as a portable radio telephone or a handheld computer suitably adapted to implement said method.

Portable radio telephone, or "mobile phone", ownership during recent years has been well documented and reported world-wide. Whilst mobile phone networks such as the Global System for Mobile communications (GSM) were originally designed for voice traffic, the sending of text messages using a Short Messaging Service (SMS) via suitably equipped phones has risen dramatically over the past couple of years, with the number of SMS messages sent world-wide on the GSM networks reaching fifteen billion in December 2000. This is in part due to the critical mass of ownership now reached in developed countries and also due to the low and typically fixed costs of sending a text message when compared with a voice call. The popularity of text messaging is also explained by the private and often intimate communication path offered by a text message. The numbers of text messages sent and received by users are forecast to increase even further with the impending introduction of more advanced, so-called 3G (third generation) wireless networks and services, where data, fax and more advanced e-mail services will be available on a 3G mobile phone or suitably equipped handheld computer or personal digital assistant (PDA).

A known method of entering text into devices such as mobile phones involves a user pressing a key on a keypad several times to cycle through characters associated with the key, until the character required is selected. For example, the number "2" key is associated with the characters "abc", the "3" key with the characters "def", the "4" key with the characters "ghi", the "5" key with "jkl" and so on. To select the character "a", the "2" key is pressed once. To select the character "b" the "2" key is press twice. The character "1" is selected by pressing the "5" key three times and so forth. Special characters (for example full stop, exclamation mark, double quote, dollar, percent, ampersand and star) are produced by tapping the one or zero keys several times until the required special character is selected. This method of entering text, commonly referred to as the "multitap" method is at present almost ubiquitous on mobile phones due to agreed standardisation between mobile phone manufacturers and service providers. Users are therefore very familiar with the multitap keypad layout and character association. However, this method often requires more than two key taps to select a character, and the entering of special characters can take many key taps. The method is therefore slow and prone to error.

An alternative method of inputting text to a device is disclosed in U.S. Pat. No. 5,128,672 wherein the device comprises a dynamic predictive keyboard which is graphically represented on a touch sensitive display. A user inputs a character by pressing a key with the required character displayed on it. Following a character input, software provided within the device formulates a prediction, based on statistical analysis of the make-up and composition of English words of the next most likely character required by the user and consequently the layout of the keyboard is altered such that said most likely character is displayed on the keyboard. This has the problem that the keyboard does not resemble the multitap keypad familiar to mobile phone users, thereby presenting an unfamiliar interface to the average user. This problem is further compounded since in use the constant changing of the keyboard layout necessitates much practice and learning for proficient and quick text entry. Furthermore, the access and input of special characters is a problem unsolved by the predictive means of U.S. Pat. No. 5,128,672.

It is therefore an aim of the present invention to provide an improved method of entering characters into a device such as a mobile phone or handheld computer. It is a further aim of the present invention to provide a method consistent with a keypad with which mobile phone users are familiar.

According to a first aspect of the present invention there is provided a method for inputting a character to a device, the device comprising a keypad, the keypad comprising a plurality of keys, at least one of which keys has a primary character, a plurality of secondary characters and a display area associated with it, the keypad in a default state displaying the primary character associated with a key in its respective display area, wherein the method comprises the steps of: detecting a first key selection; displaying each of the secondary characters associated with the first selected key in a respective display area; detecting a second key selection; selecting for input the secondary character associated with the second key selection; and returning the keypad to the default state.

According to a second aspect of the present invention there is provided a device for receiving character input, comprising a keypad having a plurality of keys, a key having a primary character, a plurality of secondary characters and a display area associated with it, wherein means are provided for displaying in a default state the primary character associated with a key in its respective display area, means responsive to a first key selection are provided for displaying each of the secondary characters associated with the selected key in a respective display area, and means responsive to a second key selection are provided for selecting as input character the secondary character associated with the second key selected and for returning the keypad to its default state.

The device and method of this invention comprise a keypad having a default display state wherein primary, and optionally secondary, characters are displayed. A user inputs a character by selecting the key having that character as one of its associated secondary characters, following which the keypad displays the required character which is then input via an appropriate second key selection.

In one embodiment of the present invention the keypad is displayed on a touch screen, the touchscreen having an output area for displaying characters input by the user. In this embodiment the display area associated with a key is provided by an area of touchscreen within or adjacent to the graphical representation of the key or button.

In another embodiment of the present invention the associated display area of a key is provided by display means such as a liquid crystal display within or adjacent to the key or button. The display means are arranged such that a displayed character is visible to the user, and hence character association with the key is rendered obvious to the user.

The method and device of this invention provide improved text entry particularly suited to, but not exclusively for, hand held devices such as portable mobile radio telephones, personal digital assistants, pocket computers and remote control handsets.

Embodiments of the present invention will now be described, by way of example only, with reference to the accompanying figures in which:

FIG. **1** depicts a default display state of a keypad for use with the present invention.

FIG. **2** illustrates an example of the characters displayed on the keypad after a first key selection.

FIG. **3** depicts an example of a device made in accordance with the present invention.

FIG. **4** is a schematic diagram of components of the device of FIG. **3**.

FIG. **5** is a flow diagram illustrating a basic implementation of a method according to the present invention.

FIG. **6** depicts an alternative default display state of a keypad for use with the present invention.

In the figures the same reference numerals have been used to indicate corresponding features.

FIG. **1** depicts a keypad **100** in a default display state wherein twelve keys **102** are arranged in four rows of three keys. Each key has a primary character **104** and a plurality of secondary characters **106** associated with it. The primary character **104** displayed on each key **102** is, in this embodiment, selected from the group of characters 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, # and *. The secondary characters **106** associated with each key are shown in groups adjacent the respective key. The secondary character groupings in this embodiment are similar to those of the multitap method, for example the key associated with primary character “2” has an associated secondary character grouping “abc”, the key “3” the associated secondary characters “def” and so on as shown in the figure. Hence, the default display state of the keypad **100** as shown in FIG. **1** presents to the user a keypad having a well known key and character layout, thereby necessitating little or no familiarisation.

FIG. **2** illustrates a possible display state of the keypad **100** after a first key selection by a user, the selected key in this example being the “5” key (the key associated with the primary character “5” and secondary characters “jkl”). The secondary character “j” is displayed by the display area associated with a neighbouring key, in this example the key associated with the primary character “4” adjacent the “5” key. Similarly, the secondary characters “k” and “l”, associated with the first key selection, are displayed respectively on the keys previously displaying “2” and “6” as primary characters. In this example the remaining keys have displayed upon them further characters **200** which are useful for text entry. For example characters representing an exclamation mark, a double quote, a pound, a dollar sign, left and right brackets, a percentage symbol and a caret may be displayed as shown in FIG. **2**.

A second key selection from the keypad of FIG. **2** selects the character displayed on the display area associated with said second key for input. Following a character input, the keypad of FIG. **2** is returned to the default display state as shown in FIG. **1**.

The key selections are typically provided by a user’s finger or stylus and may comprise the user tapping a first key followed by the user tapping a second key. Alternatively, the user may make a second key selection by sliding or dragging said finger or stylus across the keypad from the first key to the second key and pausing on, or removing the finger or stylus from, the required second key.

The dynamic keypad states illustrated in FIG. **1** and FIG. **2** provide a method of quick and accurate character input wherein secondary characters are available with only two key selections. Additionally the method is intuitive and requires little or no learning by the user due to the provision of a familiar default keypad display state.

An embodiment of a device employing the keypad and features of this method and made in accordance with the present invention is shown in FIG. **3**. The figure depicts a hand-held device **300** such as a personal digital assistant (PDA) or sometimes called a handheld computer. The device comprises a touchscreen **302** comprising touch input means arranged to detect touch input upon a surface of a display means (such as a liquid crystal or organic light emitting diode display). The touchscreen in this embodiment displays a keypad **100** to the user within a touch input region **302**a of the touchscreen, whilst input characters **304** are displayed in an output region **302**b of the touchscreen **302**. In FIG. **3** the keypad **100** is shown in the second display state of FIG. **2**, wherein a first key selection of the key “5” has occurred and the keypad awaits a second key selection to input a character. The device further comprises control buttons **306** provided to power up the device or change mode of usage for example. Additionally the handheld device may incorporate means (not shown on FIG. **3**) to transmit and receive data including voice and text messaging wirelessly via a suitable network.

The device **300** further comprises components adapted for carrying out a method in accordance with the present invention, these components being schematically represented in FIG. **4**. The relevant components comprise a computer program (PRG) and processing means in the form of a general purpose microprocessor **400** (μP). The computer program is stored in computer readable storage media **402** (MEM), the PRG comprising instructions to instruct the microprocessor (μP) **400** to carry out the steps of a method according to the present invention. It is noted herewith that although the processing means of this embodiment comprise a general purpose microprocessor, other suitable forms of processing means such as dedicated logic circuits, PICmicro® chips or application specific integrated circuits (ASIC) operating with or without a computer program could be employed in alternative embodiments.

In FIG. **4** there is also provided the touchscreen **302**, the touchscreen able to display a keypad **100** (KP) and detect touch input for inputting characters. In this embodiment the display area associated with each key **102** of the keypad **100** is provided by an area of touchscreen **302** within or adjacent to the graphical representation of the key **102**. p Additionally, one or more key character tables (KCT) are provided within MEM **402**. A KCT provides information to the microprocessor relating to the default keypad to be displayed on the touchscreen, and also provides the primary and secondary characters which are to be displayed upon a first key selection.

An example of a KCT is presented below (Table 1).

TABLE 1

KEY	PRIMARY CHARACTER	SECONDARY CHARACTER(S)
1	1	Not used
2	2	abc
3	3	def
4	4	ghi
5	5	jkl
6	6	mno
7	7	pqrs

TABLE 1-continued

KEY	PRIMARY CHARACTER	SECONDARY CHARACTER(S)
8	8	tuv
9	9	wxyz
0	0	Not used
*	*	Not used
#	#	Not used

Table 1 thereby provides primary and secondary characters to the microprocessor which, under the guidance of PRG instructs the touchscreen to display these characters in the appropriate locations to build up a default keypad display state corresponding to FIG. **1** and Table 1.

Similarly a KCT relating to a first key selection of key 5 is shown below in Table 2.

TABLE 2

KEY	DISPLAY SECONDARY CHARACTER
1	!
2	k
3	"
4	j
5	5
6	1
7	£
8	$
9	%
0	ˆ
*	(
#	)

This KCT provides the characters displayed upon a first key selection corresponding to key 5 thereby providing a second keypad display state as shown in FIG. **2**.

In operation, the microprocessor **400**, under the guidance of PRG looks up the default key character assignations stored in MEM **402** as a KCT (for example the KCT of Table 1) and instructs the touchscreen **302** to display the keypad **100** in a default display state. The touchscreen is sampled repeatedly until a first key selection is detected, following which the appropriate characters to be displayed are retrieved from an appropriate stored KCT (e.g. Table 2) by the microprocessor and provided to the touchscreen which updates the keypad **100** displayed. Following these operations the touchscreen is sampled repeatedly for a second key selection.

Upon detection of a second key selection the microprocessor **400** compares the key selected with the displayed KCT (Table 2 for example) and returns the input character for display in the output region **302**b of the touchscreen **302**. Finally, the microprocessor instructs the touchscreen to display the default keypad and awaits further user interaction.

A flow diagram illustrating the main steps of this method is presented in FIG. **5**, the method being performed as a loop, wherein:

A default keypad is displayed (DIS DEF KP) **502**

The keypad is monitored for a first key selection (MON1) **504**

Following a first key selection the appropriate characters are displayed on the keypad (DIS 2^{nd} KP) **506**

The keypad is monitored for a second key selection (MON2) **508**

Following a second key selection the secondary character associated with the second key selection is returned as an input character (RET CHAR) **510**

Loop back to display the default keypad (DIS DEF KP) **502**

In a further embodiment, the first key selection is reported only after the key is selected by a user for a pre-determined time period, for example a time period of 0.2 seconds. This enables quick tapping to select the default primary characters displayed on a default keypad, thereby allowing fast number entry when required without altering the keypad display state.

According to a further embodiment of this invention, the display of primary or secondary characters associated with a key is achieved by providing an associated display area within, on or situated adjacent to the key. The default assigned secondary characters are provided adjacent to the keys on the keypad, and the user presses the keys to input characters in accordance with a method of this invention.

In a further embodiment of this invention, the default display state of the keypad comprises positioning some of the secondary characters associated with a key such that the key display area upon which a secondary character will be displayed next is indicated to the user. An example of a keypad default display state according to this embodiment is given in FIG. **6** wherein secondary characters are displayed within a key, each secondary character being positioned relative to the key upon which it will appear following a first key selection. For example, the key displaying the primary character “5” has the secondary characters “j”, “k” and “l” positioned to the left, above and right of the “5” respectively. Hence a visual indication of the key upon which each character will appear should the “5” be first selected is provided to the user. In this example the default display state provides an indication that the “j” will appear on the “4” key to the left of the “5” key, as is shown in the example of the keypad in FIG. **2**.

In yet a further embodiment of this invention, one or more of the key character tables are alterable, thereby providing a user with the option of customising the keypad to his or her preference.

Whilst the embodiments described hereinbefore apply this invention to handheld devices such as PDAs and mobile phones, it will be apparent to those skilled in the art that the teaching of this invention may also be applied to advantage to devices wherever character input is required, such as remote control handsets or children’s learning aids and toys.

Additionally, the characters assigned as primary and or secondary characters may be any characters convenient for the device, language and application chosen, and the keypad may comprise more or less keys displaying more or less characters than those illustrated herein without departing from the spirit and scope of this invention.

What is claimed is:

1. A method for inputting a character to a device, the device [comprising] *including* a keypad, the keypad [comprising] *including* a plurality of keys, at least one of [which] *the* keys has a primary character, a plurality of secondary characters and [a] *an associated* display area [associated with it], the keypad in a default state displaying the primary character associated with [a] *the at least one* key in [its respective] *the associated* display area, [wherein] the method [comprises the steps] *comprising acts* of:

in the default state,

returning the primary character as an input character in response to selection of the at least one key for a period shorter than a predetermined time period;

switching to a second state after detecting a first key selection *of the at least one key for a period longer than the predetermined time period*;

in the second state

displaying each of the secondary characters associated with the first selected key in a respective display area;

detecting a second key selection;

selecting for *the* input *character* the secondary character associated with the second key selection; and

returning the keypad to the default state.

2. [A] *The* method according to claim **1**, [wherein the keypad in a default state] further [displays] *comprising an act of displaying by the keypad in the default state* associated secondary characters adjacent the primary character, the location of each secondary character providing an indication of which display area will display that secondary character following a first key selection.

3. A computer program product stored on a computer readable *non-transitory* medium [for performing all of the steps of claim **1**] *that* when [the program is] run on a device for receiving character input *including a keypad, the keypad including a plurality of keys, at least one of the keys having a primary character, a plurality of secondary characters and an associated display area, the keypad in a default state displaying the primary character associated with the at least one key in the associated display area, performs acts of:*

in the default state,

returning the primary character as an input character in response to selection of the at least one key for a period shorter than a predetermined time period;

switching to a second state after detecting a first key selection of the at least one key for a period longer than the predetermined time period;

in the second state,

displaying each of the secondary characters associated with the first selected key in a respective display area;

detecting a second key selection;

selecting for the input character the secondary character associated with the second key selection; and

returning the keypad to the default state.

4. A device for receiving character input, comprising*:*

a keypad having a plurality of keys, at least one of which keys has a primary character, a plurality of secondary characters and [a] *an associated* display area [associated with it, wherein]*:*

means [are provided] for displaying in a default state the primary character associated with [a] *the at least one* key in [its respective] *the associated* display area[,]*;*

in the default state,

means for returning the primary character as an input character in response to selection of the at least one key for a period shorter than a predetermined time period;

means *for switching to a second state* responsive to a first key selection [are provided] *of the at least one key for a period longer than the predetermined time period;*

in the second state,

means for displaying each of the secondary characters associated with the selected key in a respective display area[, and]*;*

means responsive to a second key selection [are provided] for selecting as *the* input character the secondary character associated with the second key selection*;* and

means for returning the keypad to [its] *the* default state.

5. [A] *The* device as claimed in claim **4**, further comprising a touchscreen on which the keypad is displayed and wherein the display area associated with [a] *the at least one* key comprises a respective portion of the touchscreen.

6. [A] *The* device as claimed in claim **4**, [wherein] *comprising a display means within the key for displaying* the display area associated with [a] *the at least one* key [is provided by display means within the key].

7. [A] *The* device as claimed in claim **4**, [wherein] *comprising a display means adjacent the key for displaying* the display area associated with [a] *the at least one* key [is provided by display means adjacent the key].

8. The device as claimed in claim 4, wherein the means for switching to a second state comprises a means for detecting a sliding across the keypad from the first key selection to the second key selection.

9. The method as claimed in claim 1, the device further including a touchscreen, the method comprising an act of displaying the keypad and the at least one key on the touchscreen.

10. The method as claimed in claim 1, the device further including a display within the at least one key, the method comprising an act of displaying the display area associated with the at least one key on the display.

11. The method as claimed in claim 1, the device further including a display adjacent the key, the method comprising an act of displaying the display area associated with the at least one key on the display.

12. The method according to claim 1, wherein the act of detecting the second key selection comprises an act of detecting a sliding across the keypad from the first key selection to the second key selection.

13. The computer program product as claimed in claim 3, the device further including a touchscreen, the method comprising an act of displaying the keypad and the at least one key on the touchscreen.

14. The computer program product as claimed in claim 3, the device further including a display within the at least one key, the method comprising an act of displaying the display area associated with the at least one key on the display.

15. The computer program product as claimed in claim 3, the device further including a display adjacent the key, the method comprising an act of displaying the display area associated with the at least one key on the display.

16. The computer program product as claimed in claim 3, wherein the act of detecting the second key selection comprises an act of detecting a sliding across the keypad from the first key selection to the second key selection.

* * * * *

2

US006690387B2

(12) United States Patent

Zimmerman et al.

(10) Patent No.: US 6,690,387 B2

(45) Date of Patent: Feb. 10, 2004

(54) **TOUCH-SCREEN IMAGE SCROLLING SYSTEM AND METHOD**

(75) Inventors: **John Zimmerman**, Ossining, NY (US); **Jacquelyn Annette Martino**, Cold Spring, NY (US)

(73) Assignee: **Koninklijke Philips Electronics N.V.**, Eindhoven (NL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 214 days.

(21) Appl. No.: **10/034,375**

(22) Filed: **Dec. 28, 2001**

(65) **Prior Publication Data**

US 2003/0122787 A1 Jul. 3, 2003

(51) **Int. Cl.**^{7} **G09G 5/00**

(52) **U.S. Cl.** **345/684**; 345/784; 345/682

(58) **Field of Search** 345/173, 672, 345/676, 680–682, 684, 687, 688, 784, 785

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,075,673 A	*	12/1991	Yanker	345/163
5,526,023 A	*	6/1996	Sugimoto et al.	345/173
5,850,211 A	*	12/1998	Tognazzini	345/158
5,864,330 A	*	1/1999	Haynes	345/856
6,384,845 B1	*	5/2002	Takaike	345/786

* cited by examiner

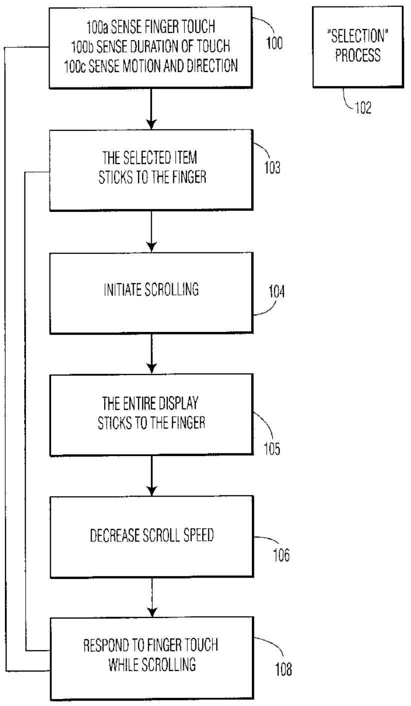
Primary Examiner—Kent Chang

(74) *Attorney, Agent, or Firm*—Aaron Waxler

(57) **ABSTRACT**

Electronic image displays. of lists that extend beyond the vertical display dimension of the display screen, are displaced in the vertical direction by touching the screen with a finger and then moving the finger in the desired direction on the screen. In a natural manner the initial speed of displacement of the displayed image corresponds to the speed of motion of the finger along the screen. When the user's finger is disengaged from the screen, the system senses the disengagement and thereafter allows the vertical displacement speed of the image to decrease at a controlled rate. When it is desired to stop the motion of the image at a given point, or to make a selection from the displayed image, the system measures the length of time that the finger is in contact with the screen and the distance that the finger is moved during that time, to determine if a selection is desired or if it is desired only to stop displacement of the image. That is, a short term contact with the screen, say 500 ms or less, accompanied by little or no displacement on the screen, can be identified as an intended selection. while a longer contact with little or no accompanying displacement can be interpreted as being intended to stop the motion of the image without making a selection.

12 Claims, 2 Drawing Sheets


100a SENSE FINGER TOUCH
100b SENSE DURATION OF TOUCH
100c SENSE MOTION AND DIRECTION
100
"SELECTION" PROCESS
102
THE SELECTED ITEM STICKS TO THE FINGER
103
INITIATE SCROLLING
104
THE ENTIRE DISPLAY STICKS TO THE FINGER
105
DECREASE SCROLL SPEED
106
RESPOND TO FINGER TOUCH WHILE SCROLLING
108

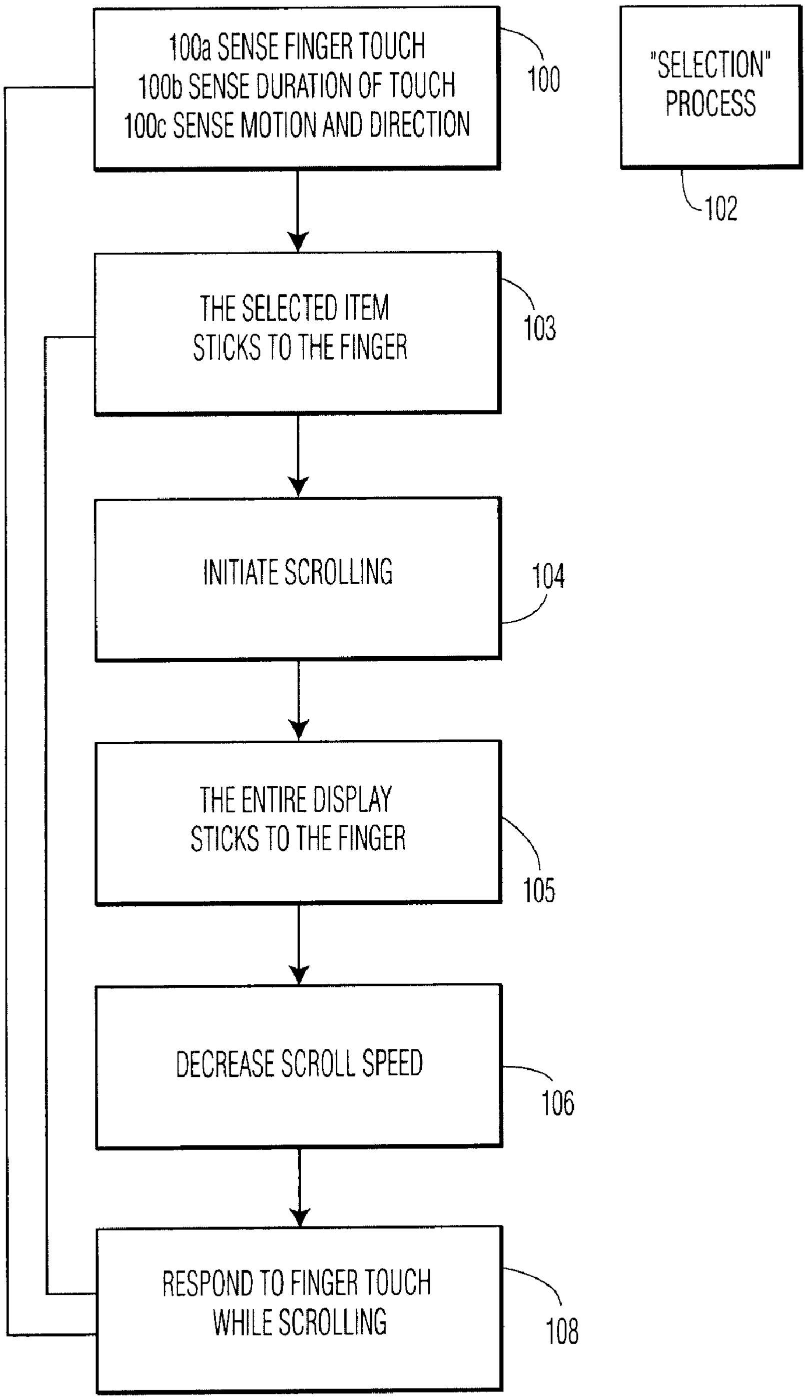

100a SENSE FINGER TOUCH
100b SENSE DURATION OF TOUCH
100c SENSE MOTION AND DIRECTION
100
"SELECTION" PROCESS
102
THE SELECTED ITEM STICKS TO THE FINGER
103
INITIATE SCROLLING
104
THE ENTIRE DISPLAY STICKS TO THE FINGER
105
DECREASE SCROLL SPEED
106
RESPOND TO FINGER TOUCH WHILE SCROLLING
108

FIG. 1

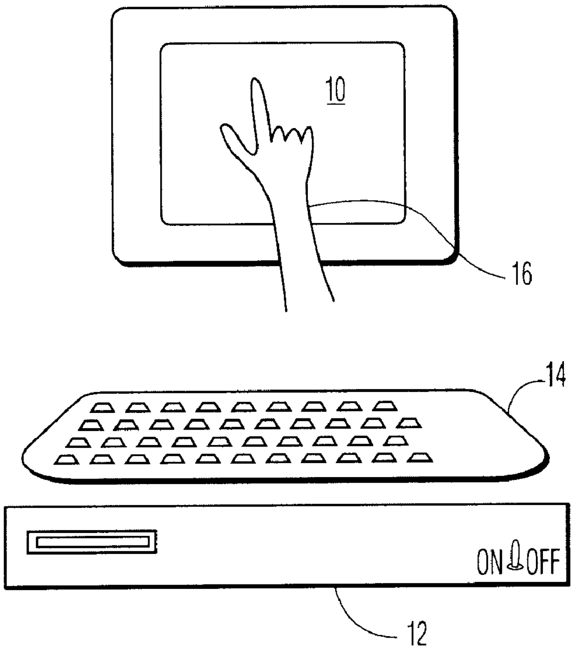

10
16
14
ON
OFF
12

FIG. 2

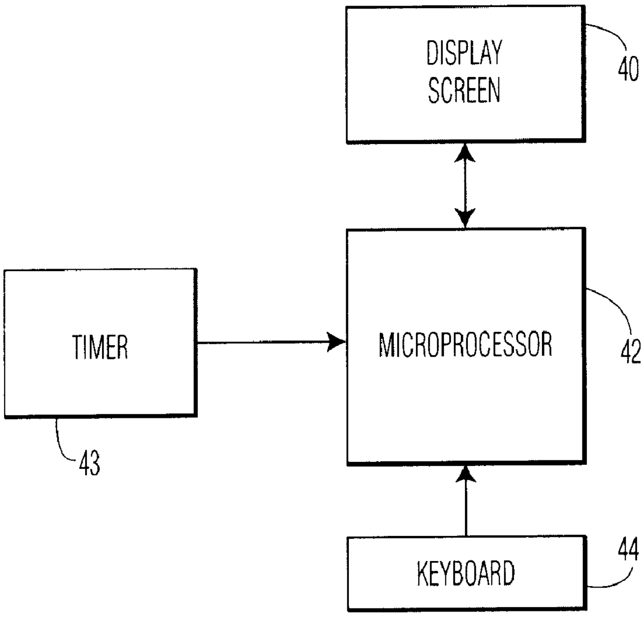

DISPLAY SCREEN
40
TIMER
MICROPROCESSOR
42
43
KEYBOARD
44

FIG. 3

TOUCH-SCREEN IMAGE SCROLLING SYSTEM AND METHOD

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to displays of information data in the form of sequential lines of symbols commonly comprising lists of words and numbers, and more specifically relates to the use and control of electronic forms of such displays.

2. Description of the Related Art

It has become well-known to display lists of words and numbers on electronic display screens for ready access by users. Often, such lists extend in length beyond the dimensions of the electronic screen, and in such cases it has further become well-known to cause the image of the list to "scroll" past the screen so that a line of text comprising words, numbers or other symbols, appears to travel from one edge of the screen to the other until a desired section of the list, or portion of a line, appears on the screen.

It is known that the systems and methods currently being used to control the scrolling motion of the screen image are subject to numerous limitations and disadvantages. For example, in one system a cursor may be positioned at one edge of the screen and then moved toward the opposite edge while holding down a selected "mouse" button, thereby engaging and "dragging" the screen image in a desired direction. It is well known that such displacement of the screen image is slow and cumbersome except for relatively slight relative movements. Another system in current use activates an automatic continuous "scrolling" motion of the image when the cursor is positioned on a specific portion of the image, while a selected mouse button is depressed. This requires holding down the selected button until the desired portion of the screen image is displayed. A related system in current use varies the speed of the scrolling motion in accordance with the position of the cursor relative to the edge of the screen. All of these cursor position-responsive control systems are subject to similar limitations of screen clutter, lack of aesthetic visual appeal, and the requirement for manipulation and handling of the mouse device.

SUMMARY OF THE INVENTION

The invention herein disclosed improves upon the scroll-like display of data on electronic display screens by making it possible for a user/viewer to access a desired portion of a long list of data and information by scrolling to the location of that portion rapidly and in a more natural manner than heretofore possible.

The present invention overcomes and avoids the limitations of known control systems for scrolling electronic displays by providing a touch-screen responsive system that imparts a scrolling motion to the displayed image in response to the motion of a finger in contact with the screen. The speed and direction of motion of the finger along the screen determines the initial speed and direction of motion for the image. After the finger separates from the screen, the image continues to move in the same direction at a gradually decreasing speed until motion is stopped manually by touching the screen without movement of the finger, or the speed decreases to zero, or to a predetermined minimum speed, or until the image reaches its "end". Alternatively, continued motion of the image may be achieved or again increased by repeating the "sweeping motion" of a the user's finger along the screen. Motion of the displayed image may be stopped manually by applying a finger to the screen without moving it along the surface of the screen for a finite period of time. If a finger is applied to the surface of the screen for a shorter period of time, for example for a period less than a minimum set time, the finger touch can be deemed to be a "selection" of an item or "thing" corresponding to the image displayed at the touched location. Still further, if the finger touch on the screen is made to move with the display, but at a slower rate than the then-current rate of movement, the display will be slowed to a rate corresponding to the motion of the finger at the movement that contact is broken.

This operation of the system of this invention is achieved by programming a microprocessor-based control system to displace the image on a screen display, such as the screen of a conventional cathode ray tube, in response to a finger touch on the screen and the direction of a finger motion along the surface of the screen at the initial speed of the finger motion. Thereafter, the speed of displacement is caused to decay at a selected rate (units of displacement per unit of time, or a function thereof), until the displacement finally stops (for example, due to having reached the end of the "scroll") or until it is stopped deliberately as explained herein.

In accordance with this invention, the scrolling motion of data on the display screen moves in a seemingly "natural" way, moving initially at a speed imparted by the motion of the user's finger, with the speed thereafter slowing at a constant rate until it ultimately comes to rest, unless it is terminated earlier.

Moreover, if the speed of scrolling is found to be slow at a point deemed to be too far before the desired location in the scroll, the scrolling speed may be increased as many times as possible by merely touching the screen again to impart "new" motion to the display.

At any desired point or time while a scrolling motion is in progress, it may be stopped entirely, again in a seemingly "natural" way, by merely touching one's finger to the screen while holding it substantially stationary for a predetermined period of time. The reason for requiring a predetermined time-period for stationary [i.e. no-motion] touch time is to assure that the timing mechanisms will have sufficient time to distinguish between a touch intended to stop the scrolling motion and a touch [shorter in time] intended to "select" or "mark" a particular item that is included in the scrolled data. "Touch marking" is a well-known feature of scrolled display technology at this time, but this invention discloses its use in combination with a new, and heretofore unknown, form of scrolling motion control.

These and other features and advantages of this invention will be made more apparent to those having skill in this art, by reference to the following specification considered in conjunction with the accompanying drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a flow-chart representing the sequential operations of a touch-screen image scrolling system in accordance with this invention.

FIG. **2** is simplified pictorial representation of a touch-screen image scrolling system in accordance with one embodiment of the invention of FIG. **1**.

FIG. **3** is a simplified block diagram of another embodiment of a touch-screen image scrolling system in accordance with FIG. **1**.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following description, certain specific details of the disclosed embodiment such as architecture, interfaces and techniques, etc, are set forth for purposes of explanation rather than limitation, so as to provide a clear and thorough understanding of the present invention. However, it should be understood readily by those skilled in this art, that the present invention may be practiced in other embodiments which do not conform exactly to the details set forth herein, without departing significantly from the spirit and scope of this disclosure. Further, in this context, and for the purposes of brevity and clarity, detailed descriptions of well-known apparatus, circuits and methodology have been omitted so as to avoid unnecessary detail and possible confusion.

Referring now to the block diagram of FIG. **1** of the drawings, the method of operating a touch-screen image scrolling system **10** (as shown in FIG. **1**) in accordance with this invention may be seen to begin in step **100** with sensing the touch of a finger upon an electronic display screen **100***a* having a stationary data display, determining the period of time that the finger is in contact with the screen **100***b*, and determining if the finger moves or remains stationary. **100***c*. The technology and methodology for sensing and determining the appropriate values for information of the type herein disclosed is well-known to persons having skill in this art, and is not further described or discussed in this specification.

If no motion occurs and the touch contact continues for less than a predetermined minimum time, the touch is treated in step **100** as a "selection" of the data term touched, and the system continues with "selection" path **102**. The operation of a selection path, beginning with, for example, highlighting of the term or icon touched, is well-known and is of no further concern in connection with the operation of the system of this invention. However, if the touch contact continues for more than the first predetermined minimum time, and the finger then moves after that time, the process of the invention will proceed to step **103**, in which the "selected" item on the list will then "stick to the finger" so that the item can be repositioned on the list by the known process of "touch-dragging". This repositioning step can be very desirable to frequent users who may wish to cluster several preferred items in a given location. After an item has been repositioned in step **103**, and finger contact with the screen is interrupted, the process will revert to "waiting" status. With advance reference to step **105**, explained below, it should be noted here, that in this step it is a selected item, rather than the entire display, that "sticks to the finger."

In another feature, if no motion of the finger occurs while the screen is stationary, and the contact continues for less than a second minimum time which is less than the first minimum time by a readily measurable finite value, then step **100** ignores the contact and the system reverts to "waiting" status, awaiting further input signals.

However, if step **100** senses motion in association with the finger touch on the screen, during the finite period between the first predetermined time and the second, then the method of the invention proceeds to step **104**, converting the speed and direction of motion of the touch into corresponding initial scrolling motion of the displayed data. And step **104** proceeds directly into step **106**. Step **104** either proceeds to step **106**, or diverges to step **105** depending upon whether the finger is removed from contact with the screen or continues in contact with the screen.

That is, if the finger touch of step **104** imparts movement to the display and the touch-contact is then broken, movement of the display continues in accordance with step **106**. However, if contact with the screen is not broken, the method of the invention proceeds from step **104** to step **105**, wherein the entire display [not just a selected item] in effect "sticks to the finger" so that the entire display can be moved up or down or back and forth, as the case may be, with the finger. If there is no finger motion at the time that finger contact with the screen is broken in step **105**, the display will remain in the position it is in at that time without further motion, and the system will revert again to "waiting" status. In the alternative, if finger contact in step **105** is broken while the finger is in motion, the system of the invention proceeds to step **106**, as described below.

In step **106**, the timer function associated with the system of the invention measures time while the scrolling action continues and the system begins decreasing the scrolling speed at a controlled rate, from its initial value which is determined by the speed of the finger touch, toward zero or until the speed is reduced to any desired, predetermined minimum speed. It is assumed that most users of this system will prefer that the decrease in scrolling speed begin immediately after the start of scrolling. However, it should be recognized that the start of the decreasing speed function can, in fact, be delayed so as to begin at any time after the start of the scrolling motion. Incorporating a finite-time delay into the control system for utilization of this method is a simple technique well within the knowledge of those skilled in this art.

While the slowing scrolling motion continues, and after scrolling has terminated entirely, the system continues waiting for further input signals, to control the next operation of the system. However, in accordance with the invention, slowing of the scrolling speed continues until one of three events occurs: (1) slowing decreases the speed of the scroll to zero or to any preset minimum; or (2) an "end of scroll" data signal is received from the data source; or (3) a finger touch on the screen indicates that the scrolling is to be terminated. Regardless of the status of the slowing action, the method of this invention allows the system to react to the next user-initiated input signal at any time, following step **106**.

Step **108** shows that the method of the invention reacts to a finger touch on the screen during or after scrolling by repeating, essentially, the functions of step **100**. That is, in step **108**, the system senses the touch of a finger **100***a* on the electronic display screen, determines the period of time **100***b* that the finger is in contact with the screen, and determines if the finger moves or remains stationary. **100***b*. If the touch is stationary and the contact continues for less than a predetermined minimum time, the finger touch is treated in step **108** as both (1) a "selection" of the data term touched, and (2) an instruction to terminate the scrolling motion. In this case, scrolling motion terminates and the system reverts to the "selection" path **102**, previously mentioned. On the other hand, if the touch is stationary but the contact does not continue for more than the minimum time, the method treats the touch as an instruction to terminate the scrolling motion only, and there is no resulting "selection" of any data listing that may have been touched. When scrolling motion terminates under these circumstances, the method reverts to the state that exists before the beginning of step **100**, waiting for "instructions" in the form of input signals; i.e. awaiting either selection of a displayed item or initiation of scrolling motion.

Once again it should be emphasized that the duration of contact for a stationary finger touch on the screen serves as the distinction between a "selection" touch and a "stop scrolling" touch. Although it has been stated above, that a relatively long-term finger touch while scrolling motion is taking place serves as both a "selection" and a "stop motion" signal, it will be obvious that the method could be set up easily so that a finger touch during the scrolling process would act solely as a "stop motion" signal regardless of the length of the touch; this would protect against the possibility of unintended "selections" resulting from inadvertently long touches that were intended only to "stop" the scrolling.

In contrast to stationary touching in step **108**, if the system senses motion of the finger touch on the screen, the method reverts to step **104**, again converting the speed and direction of motion of the touch into scrolling motion of the displayed data and restarting the scrolling process. As before, step **104** then proceeds directly into step **106**.

In the embodiment of the system of this invention illustrated in FIG. **2**, the system is shown to comprise a simple personal computer apparatus having a display screen **10**, a central processing unit **12** and a keyboard **14** for inputting manual instruction to the processing unit **12**. In accordance with convention, it will be understood that processing unit **12** includes an internal electronic memory unit (not shown) of conventional design and capabilities. Accordingly, for the purposes of this disclosure, the internal memory unit may be assumed to be the source of a scrollable data display capable of appearing on display screen **10** which is accessible to a hand or stylus device, here stylistically represented by the outline of a hand **16**.

In use, the computer is set up in well-known manner to display the scrollable data on screen **10**, and a hand/finger or stylus **16** is touched to the screen and moved down along the screen to impart an initial downward "scrolling" motion to the data display. Software in the computer interactively responds to the contact with the screen to create the desired displacement motion of the display and the internal timer facility now inherent in such computer apparatus, in cooperation with the programming of processing unit **12** responds to the start of motion by gradually decreasing the speed of displacement, as explained previously herein. When a desired point in the display is seen or approached, the user may apply a hand or stylus **16** to the screen to terminate the scrolling motion. Because the scrolling motion does not involve any moving parts with real or simulated mass, it is possible to stop the motion of the display instantly, without any difficulty or concern for inertial force consequences.

Accordingly, it will now be understood that the system and method of this invention facilitates a rapid, convenient and natural-feeling approach to accessing a scroll-like display of data on a computer screen.

In the embodiment represented in FIG. **3**, the system of this invention is shown to comprise the essential elements of the computer apparatus of FIG. **2** without having the configuration of a computer. That is, the basic components of the system of this invention are here show to comprise a microprocessor **42** which is in turn coupled to a keyboard **44**, a timer means **43** and a display screen **40**. Each of these components functions in the same manner as its counterparts in the embodiment of FIG. **2**, with microprocessor **42** and the associated timer means **43** together, here serving the same function as central processing unit **12** in FIG. **2**.

Although a preferred embodiment of the invention has been illustrated and described, those having skill in this art will recognize that various other forms and embodiments now may be visualized readily without departing significantly from the spirit and scope of the invention disclosed herein and set forth in the accompanying claims.

What is claimed is:

1. An improved touch-screen image scrolling system, comprising:

an electronic image display screen;

a microprocessor coupled to said display screen to display information thereon and to receive interactive signals therefrom;

timer means associated with said microprocessor to provide timing capacity therefor;

a source of scroll format data capable of display on said display screen;

a keyboard coupled to said microprocessor to provide input control signals thereto;

finger touch program instructions associated with said microprocessor for sensing the speed, direction and time duration of a finger touch contact with said display screen;

scrolling motion program instructions associated with said microprocessor responsive to said duration of said finger touch contact such that, when said duration exceeds a first given preset minimum time and is accompanied by motion along the surface of said screen followed by separation of said finger touch from said screen, a scroll format display on said screen is caused to begin to scroll in said sensed direction and at said sensed initial speed;

time decay program instructions associated with said microprocessor for reducing the rate of scrolling displacement on said display screen at a given rate until motion is terminated;

stopping motion program instructions associated with said microprocessor for terminating scrolling displacement of the image on said screen upon first occurrence of any signal in the group of signals comprising:

(a) a substantially stationary finger touch on the screen enduring for a period longer than a preset minimum time, and

(b) an end-of-scroll signal received from said scroll format data source.

2. The improved touch-screen image scrolling system of claim **1**, wherein said scrolling motion program instructions further comprise instructions to move said display in correspondence with movement of the finger touch, in response to movement following a touch having a stationary duration greater than said first preset given minimum time and less than a second given preset minimum time.

3. The improved touch-screen image scrolling system of claim **1**, wherein said scrolling motion program instructions further comprise instructions to move a touch-selected item relative to the stationary display in correspondence with movement of said finger touch, in response to motion following a touch having a stationary duration greater than said second given preset minimum time.

4. The improved touch-screen image scrolling system of claim **1**, wherein said group of signals for terminating scrolling, displacement of the image on said display screen further comprises

(a) a signal indicating that the rate of scrolling displacement on said screen has decayed to a value below a predetermined given value.

5. The improved touch-screen image scrolling system of claim **1**, wherein said microprocessor, and said timer means together comprise a processing unit of a conventional computer.

6. The improved touch-screen image scrolling system of claim **5**, wherein said source of scroll format data capable of display on said display screen comprises part of the memory of said conventional computer.

7. An improved touch-screen image scrolling system, comprising:

an electronic image display screen;

a computer apparatus coupled to said display screen to display information thereon and to receive interactive signals therefrom;

timer means within said computer apparatus to provide timing capacity therefor;

said computer apparatus having capacity to store scroll format data capable of display on said display screen;

a keyboard coupled to said computer apparatus to provide input control signals thereto;

finger touch program instructions associated with said computer apparatus for sensing the speed, direction and time duration of a finger touch contact with said display screen;

scrolling motion program instructions associated with said computer apparatus responsive to said duration of said finger touch contact such that, when said duration exceeds a preset minimum time and is accompanied by motion along the surface of said screen, a scroll format display on said screen is caused to begin to scroll in the sensed direction and at the sensed initial speed;

time decay program instructions associated with said computer apparatus for reducing the rate of scrolling displacement on said display screen at a given rate until motion is terminated;

stopping motion program instructions associated with said computer apparatus for terminating scrolling displacement of the image on said screen upon first occurrence of any signal in the group of signals comprising:

(a) a substantially stationary finger touch on the screen enduring for a period longer than a preset minimum time, and

(b) an end-of-scroll signal received from said scroll format data source.

8. An improved touch-screen image scrolling system, comprising:

an electronic image display screen;

a microprocessor coupled to said display screen to display information thereon and to receive interactive signals therefrom;

timer means associated with said microprocessor to provide timing capacity therefor;

a source of scroll format data capable of display on said display screen;

a keyboard coupled to said microprocessor to provide input control signals thereto;

finger touch program instructions associated with said microprocessor for sensing the speed, direction and time duration of a finger touch contact with said display screen;

scrolling motion program instructions associated with said microprocessor responsive to said duration of said finger touch contact such that, when said duration exceeds a first given preset minimum time, and is less than a second given preset minimum that is greater than said first minimum, and is accompanied by motion along the surface of said screen, a scroll format display on said screen is caused to begin to scroll in the sensed direction and at the sensed initial speed;

said scrolling motion program instructions further comprising instructions to move a touch-selected item relative to the stationary display in correspondence with movement of the finger touch, in response to

motion following a touch having a stationary duration greater than said second given preset minimum time;

said scrolling motion program instructions still further comprising instructions to move said display in correspondence with movement of the finger touch, in response to motion following a touch having a stationary duration greater than said first given preset minimum time and less than said second given preset minimum time;

time decay program instructions associated with said microprocessor for reducing the rate of scrolling displacement on said display screen at a given rate until motion is terminated;

stopping motion program instructions associated with said microprocessor for terminating scrolling displacement of the image on said screen upon first occurrence of any signal in the group of signals comprising:

(a) a substantially stationary finger touch on the screen enduring for a period longer than a preset minimum time, and

(b) an end-of-scroll signal received from said scroll format data source.

9. An improved method of controlling the scroll-like display of data on an electronic display screen, said method comprising the steps of:

sensing the duration of finger touch contact time with an electronic display screen having scrollable data displayed thereon;

sensing the speed and direction of motion of said finger touch contact with said display screen;

initiating scrolling motion of said scrollable data on said display screen in said sensed direction and at said sensed speed;

slowing the speed of said scrolling motion from the initiated speed thereof, at a predetermined rate; and

terminating said scrolling motion when one of the conditions comprising the following group of conditions is sensed:

(a) a substantially stationary finger touch having a finite duration is sensed;

(b) an end-of-scroll signal is sensed.

10. The improved method of controlling the scroll-like display of data on an electronic display screen, in accordance with claim **7**, wherein said group of conditions to be sensed for terminating said scrolling motion further comprises: the speed of said scrolling motion on said screen slows to a value below a predetermined given value.

11. The improved method of controlling the scroll-like display of data on an electronic display screen in accordance with claim **9**, wherein said method comprises the further step of sensing a finger touch on said screen having a duration greater than said first given preset minimum time and less than a second given preset minimum time which is greater than said first given time and then moving said display in correspondence with movement of the finger touch.

12. The improved method of controlling the scroll-like display of data on an electronic display screen. in accordance with claim **9**, wherein said method comprises the further step of sensing a stationary finger touch on said screen having a duration greater than a second preset given minimum time which is greater than said first given preset time and then moving a touch-selected item relative to the stationary display in correspondence with movement of the finger touch.

* * * * *

3

US007184064B2

(12) United States Patent
Zimmerman et al.

(10) **Patent No.: US 7,184,064 B2**

(45) **Date of Patent: *Feb. 27, 2007**

(54) **TOUCH-SCREEN IMAGE SCROLLING SYSTEM AND METHOD**

(75) Inventors: **John Zimmerman**, Ossining, NY (US); **Jacquelyn Annette Martino**, Cold Spring, NY (US)

(73) Assignee: **Koninklijke Philips Electronics N.V.**, Eindhoven (NL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 386 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **10/736,938**

(22) Filed: **Dec. 16, 2003**

(65) **Prior Publication Data**

US 2004/0125088 A1 Jul. 1, 2004

(51) **Int. Cl.**
G09G 5/00 (2006.01)

(52) **U.S. Cl.** **345/684**; 715/784; 345/682

(58) **Field of Classification Search** 715/682, 715/684, 784; 345/682, 684
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,954,967 A		9/1990	Takahashi	364/518
5,075,673 A	*	12/1991	Yanker	345/163
5,526,023 A	*	6/1996	Sugimoto et al.	345/173
5,850,211 A	*	12/1998	Tognazzini	345/158
5,864,330 A	*	1/1999	Haynes	715/856
6,384,845 B1	*	5/2002	Takaike	715/786

FOREIGN PATENT DOCUMENTS

WO	WO 9957630	11/1999

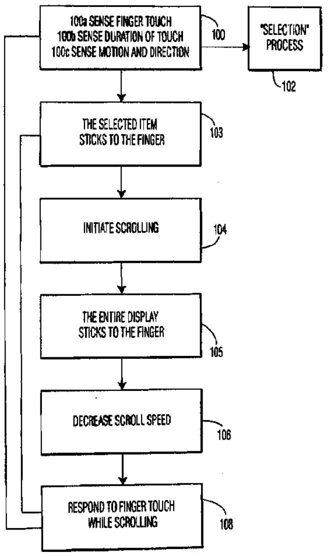
* cited by examiner

Primary Examiner—Kent Chang

(57) **ABSTRACT**

Electronic image displays, of lists that extend beyond the vertical display dimension of the display screen, are displaced in the vertical direction by touching the screen with a finger and then moving the finger in the desired direction on the screen. In a natural manner, the initial speed of displacement of the displayed image corresponds to the speed of motion of the finger along the screen. When the user's finger is disengaged from the screen, the system senses the disengagement and thereafter allows the vertical displacement speed of the image to decrease at a controlled rate. When it is desired to stop the motion of the image at a given point, or to make a selection from the displayed image, the system measures the length of time that the finger is in contact with the screen and the distance that the finger is moved during that time, to determine if a selection is desired or if it is desired only to stop displacement of the image. That is, a short term contact with the screen, say 500 ms or less, accompanied by little or no displacement on the screen, can be identified as an intended selection, while a longer contact with little or no accompanying displacement can be interpreted as being intended to stop the motion of the image without making a selection.

9 Claims, 2 Drawing Sheets


100a SENSE FINGER TOUCH
100b SENSE DURATION OF TOUCH
100c SENSE MOTION AND DIRECTION
100
"SELECTION" PROCESS
102
THE SELECTED ITEM STICKS TO THE FINGER
103
INITIATE SCROLLING
104
THE ENTIRE DISPLAY STICKS TO THE FINGER
105
DECREASE SCROLL SPEED
106
RESPOND TO FINGER TOUCH WHILE SCROLLING
108

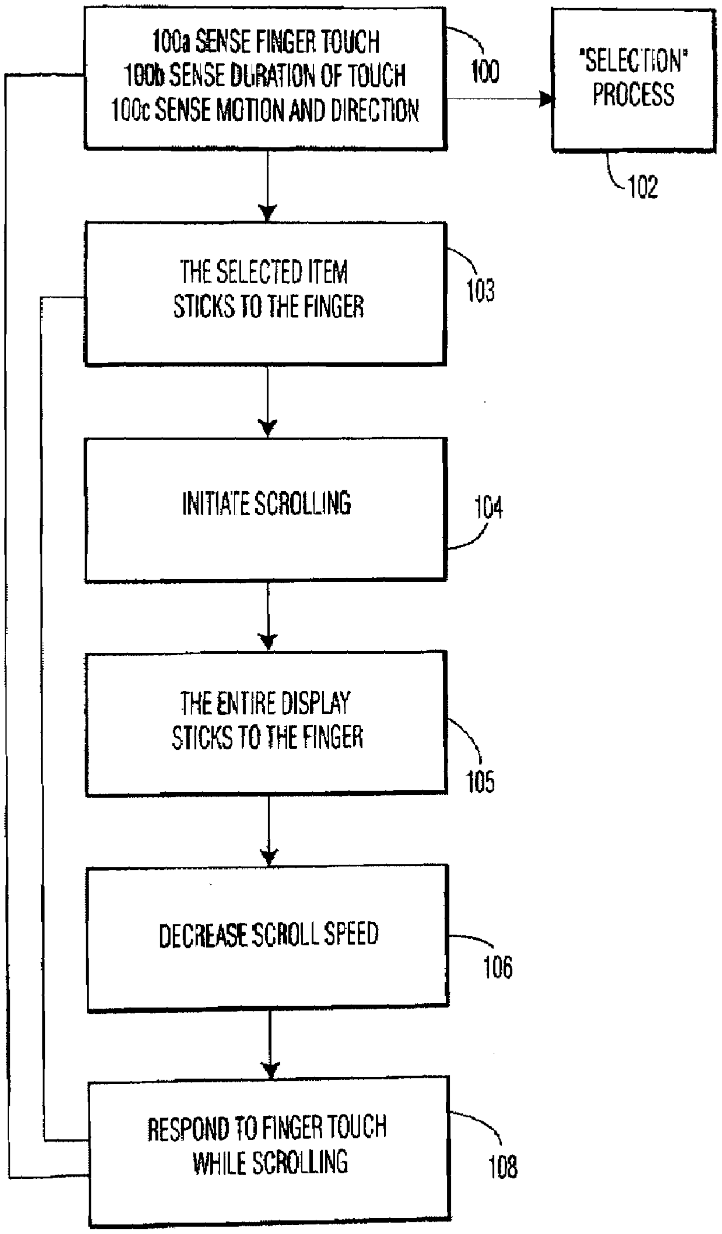

100a SENSE FINGER TOUCH
100b SENSE DURATION OF TOUCH
100c SENSE MOTION AND DIRECTION
100
"SELECTION" PROCESS
102
THE SELECTED ITEM STICKS TO THE FINGER
103
INITIATE SCROLLING
104
THE ENTIRE DISPLAY STICKS TO THE FINGER
105
DECREASE SCROLL SPEED
106
RESPOND TO FINGER TOUCH WHILE SCROLLING
108

FIG. 1

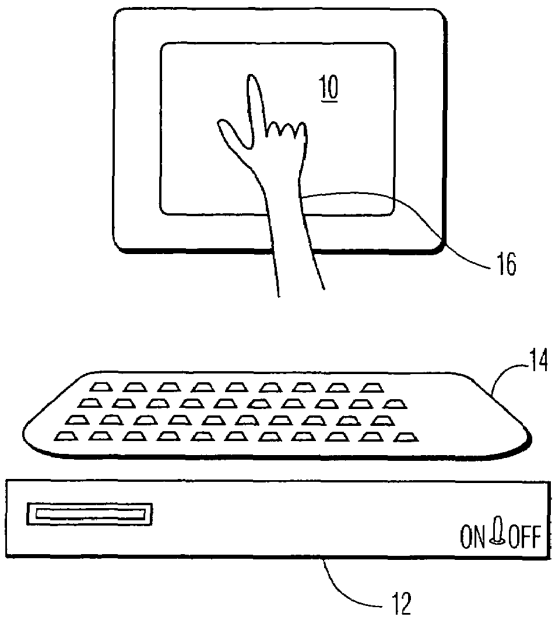

10
16
14
ON
OFF
12

FIG. 2

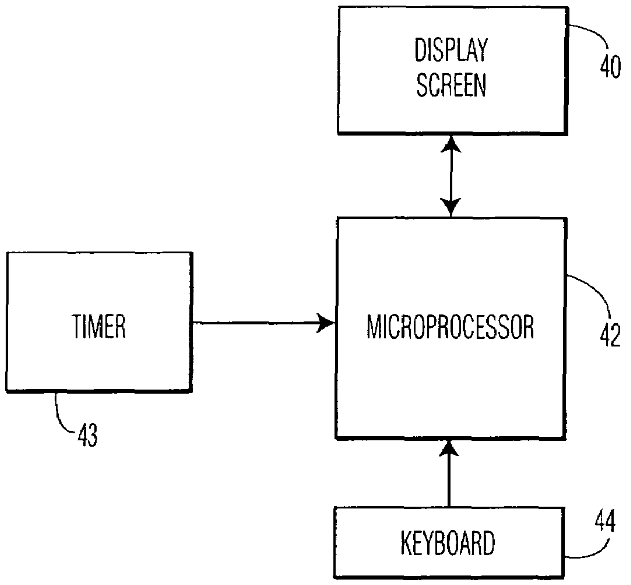

DISPLAY SCREEN
40
TIMER
MICROPROCESSOR
42
43
KEYBOARD
44

FIG. 3

TOUCH-SCREEN IMAGE SCROLLING SYSTEM AND METHOD

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to displays of information data in the form of sequential lines of symbols commonly comprising lists of words and numbers, and more specifically relates to the use and control of electronic forms of such displays.

2. Description of the Related Art

It has become well-known to display lists of words and numbers on electronic display screens for ready access by users. Often, such lists extend in length beyond the dimensions of the electronic screen, and in such cases it has further become well-known to cause the image of the list to "scroll" past the screen so that a line of text comprising words, numbers or other symbols, appears to travel from one edge of the screen to the other until a desired section of the list, or portion of a line, appears on the screen.

It is known that the systems and methods currently being used to control the scrolling motion of the screen image are subject to numerous limitations and disadvantages. For example, in one system a cursor may be positioned at one edge of the screen and then moved toward the opposite edge while holding down a selected "mouse" button, thereby engaging and "dragging" the screen image in a desired direction. It is well known that such displacement of the screen image is slow and cumbersome except for relatively slight relative movements. Another system in current use activates an automatic continuous "scrolling" motion of the image when the cursor is positioned on a specific portion of the image, while a selected mouse button is depressed. This requires holding down the selected button until the desired portion of the screen image is displayed. A related system in current use varies the speed of the scrolling motion in accordance with the position of the cursor relative to the edge of the screen. All of these cursor position-responsive control systems are subject to similar limitations of screen clutter, lack of aesthetic visual appeal, and the requirement for manipulation and handling of the mouse device.

SUMMARY OF THE INVENTION

The invention herein disclosed improves upon the scroll-like display of data on electronic display screens by making it possible for a user/viewer to access a desired portion of a long list of data and information by scrolling to the location of that portion rapidly and in a more natural manner than heretofore possible.

The present invention overcomes and avoids the limitations of known control systems for scrolling electronic displays by providing a touch-screen responsive system that imparts a scrolling motion to the displayed image in response to the motion of a finger in contact with the screen. The speed and direction of motion of the finger along the screen determines the initial speed and direction of motion for the image. After the finger separates from the screen, the image continues to move in the same direction at a gradually decreasing speed until motion is stopped manually by touching the screen without movement of the finger, or the speed decreases to zero, or to a predetermined minimum speed, or until the image reaches its "end". Alternatively, continued motion of the image may be achieved or again increased by repeating the "sweeping motion" of a the user's finger along the screen. Motion of the displayed image may be stopped manually by applying a finger to the screen without moving it along the surface of the screen for a finite period of time. If a finger is applied to the surface of the screen for a shorter period of time, for example for a period less than a minimum set time, the finger touch can be deemed to be a "selection" of an item or "thing" corresponding to the image displayed at the touched location. Still further, if the finger touch on the screen is made to move with the display, but at a slower rate than the then-current rate of movement, the display will be slowed to a rate corresponding to the motion of the finger at the movement that contact is broken.

This operation of the system of this invention is achieved by programming a microprocessor-based control system to displace the image on a screen display, such as the screen of a conventional cathode ray tube, in response to a finger touch on the screen and the direction of a finger motion along the surface of the screen at the initial speed of the finger motion. Thereafter, the speed of displacement is caused to decay at a selected rate (units of displacement per unit of time, or a function thereof), until the displacement finally stops (for example, due to having reached the end of the "scroll") or until it is stopped deliberately as explained herein.

In accordance with this invention, the scrolling motion of data on the display screen moves in a seemingly "natural" way, moving initially at a speed imparted by the motion of the user's finger, with the speed thereafter slowing at a constant rate until it ultimately comes to rest, unless it is terminated earlier.

Moreover, if the speed of scrolling is found to be slow at a point deemed to be too far before the desired location in the scroll, the scrolling speed may be increased as many times as possible by merely touching the screen again to impart "new" motion to the display.

At any desired point or time while a scrolling motion is in progress, it may be stopped entirely, again in a seemingly "natural" way, by merely touching one's finger to the screen while holding it substantially stationary for a predetermined period of time. The reason for requiring a predetermined time-period for stationary [i.e. no-motion] touch time is to assure that the timing mechanisms will have sufficient time to distinguish between a touch intended to stop the scrolling motion and a touch [shorter in time] intended to "select" or "mark" a particular item that is included in the scrolled data. "Touch marking" is a well-known feature of scrolled display technology at this time, but this invention discloses its use in combination with a new, and heretofore unknown, form of scrolling motion control.

These and other features and advantages of this invention will be made more apparent to those having skill in this art, by reference to the following specification considered in conjunction with the accompanying drawings, in which:

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a flow-chart representing the sequential operations of a touch-screen image scrolling system in accordance with this invention.

FIG. **2** is simplified pictorial representation of a touch-screen image scrolling system in accordance with one embodiment of the invention of FIG. **1**.

FIG. **3** is a simplified block diagram of another embodiment of a touch-screen image scrolling system in accordance with FIG. **1**.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following description, certain specific details of the disclosed embodiment such as architecture, interfaces and techniques, etc, are set forth for purposes of explanation rather than limitation, so as to provide a clear and thorough understanding of the present invention. However, it should be understood readily by those skilled in this art, that the present invention may be practiced in other embodiments which do not conform exactly to the details set forth herein, without departing significantly from the spirit and scope of this disclosure. Further, in this context, and for the purposes of brevity and clarity, detailed descriptions of well-known apparatus, circuits and methodology have been omitted so as to avoid unnecessary detail and possible confusion.

Referring now to the block diagram of FIG. **1** of the drawings, the method of operating a touch-screen image scrolling system **10** (as shown in FIG. **1**) in accordance with this invention may be seen to begin in step **100** with sensing the touch of a finger upon an electronic display screen **100***a* having a stationary data display, determining the period of time that the finger is in contact with the screen **100***b*, and determining if the finger moves or remains stationary **100***c*. The technology and methodology for sensing and determining the appropriate values for information of the type herein disclosed is well-known to persons having skill in this art, and is not further described or discussed in this specification.

If no motion occurs and the touch contact continues for less than a predetermined minimum time, the touch is treated in step **100** as a "selection" of the data term touched, and the system continues with "selection" path **102**. The operation of a selection path, beginning with, for example, highlighting of the term or icon touched, is well-known and is of no further concern in connection with the operation of the system of this invention. However, if the touch contact continues for more than the first predetermined minimum time, and the finger then moves after that time, the process of the invention will proceed to step **103**, in which the "selected" item on the list will then "stick to the finger" so that the item can be repositioned on the list by the known process of "touch-dragging". This repositioning step can be very desirable to frequent users who may wish to cluster several preferred items in a given location. After an item has been repositioned in step **103**, and finger contact with the screen is interrupted, the process will revert to "waiting" status. With advance reference to step **105**, explained below, it should be noted here, that in this step it is a selected item, rather than the entire display, that "sticks to the finger."

In another feature, if no motion of the finger occurs while the screen is stationary, and the contact continues for less than a second minimum time which is less than the first minimum time by a readily measurable finite value, then step **100** ignores the contact and the system reverts to "waiting" status, awaiting further input signals.

However, if step **100** senses motion in association with the finger touch on the screen, during the finite period between the first predetermined time and the second, then the method of the invention proceeds to step **104**, converting the speed and direction of motion of the touch into corresponding initial scrolling motion of the displayed data. And step **104** proceeds directly into step **106**. Step **104** either proceeds to step **106**, or diverges to step **105** depending upon whether the finger is removed from contact with the screen or continues in contact with the screen.

That is, if the finger touch of step **104** imparts movement to the display and the touch-contact is then broken, movement of the display continues in accordance with step **106**. However, if contact with the screen is not broken, the method of the invention proceeds from step **104** to step **105**, wherein the entire display [not just a selected item] in effect "sticks to the finger" so that the entire display can be moved up or down or back and forth, as the case may be, with the finger. If there is no finger motion at the time that finger contact with the screen is broken in step **105**, the display will remain in the position it is in at that time without further motion, and the system will revert again to "waiting" status. In the alternative, if finger contact in step **105** is broken while the finger is in motion, the system of the invention proceeds to step **106**, as described below.

In step **106**, the timer function associated with the system of the invention measures time while the scrolling action continues and the system begins decreasing the scrolling speed at a controlled rate, from its initial value which is determined by the speed of the finger touch, toward zero or until the speed is reduced to any desired, predetermined minimum speed. It is assumed that most users of this system will prefer that the decrease in scrolling speed begin immediately after the start of scrolling. However, it should be recognized that the start of the decreasing speed function can, in fact, be delayed so as to begin at any time after the start of the scrolling motion. Incorporating a finite-time delay into the control system for utilization of this method is a simple technique well within the knowledge of those skilled in this art.

While the slowing scrolling motion continues, and after scrolling has terminated entirely, the system continues waiting for further input signals, to control the next operation of the system. However, in accordance with the invention, slowing of the scrolling speed continues until one of three events occurs: (1) slowing decreases the speed of the scroll to zero or to any preset minimum; or (2) an "end of scroll" data signal is received from the data source; or (3) a finger touch on the screen indicates that the scrolling is to be terminated. Regardless of the status of the slowing action, the method of this invention allows the system to react to the next user-initiated input signal at any time, following step **106**.

Step **108** shows that the method of the invention reacts to a finger touch on the screen during or after scrolling by repeating, essentially, the functions of step **100**. That is, in step **108**, the system senses the touch of a finger **100***a* on the electronic display screen, determines the period of time **100***b* that the finger is in contact with the screen, and determines if the finger moves or remains stationary. **100***b*. If the touch is stationary and the contact continues for less than a predetermined minimum time, the finger touch is treated in step **108** as both (1) a "selection" of the data term touched, and (2) an instruction to terminate the scrolling motion. In this case, scrolling motion terminates and the system reverts to the "selection" path **102**, previously mentioned. On the other hand, if the touch is stationary but the contact does not continue for more than the minimum time, the method treats the touch as an instruction to terminate the scrolling motion only, and there is no resulting "selection" of any data listing that may have been touched. When scrolling motion terminates under these circumstances, the method reverts to the state that exists before the beginning of step **100**, waiting for "instructions" in the form of input signals; i.e. awaiting either selection of a displayed item or initiation of scrolling motion.

Once again it should be emphasized that the duration of contact for a stationary finger touch on the screen serves as the distinction between a "selection" touch and a "stop scrolling" touch. Although it has been stated above, that a relatively long-term finger touch while scrolling motion is taking place serves as both a "selection" and a "stop motion" signal, it will be obvious that the method could be set up easily so that a finger touch during the scrolling process would act solely as a "stop motion" signal regardless of the length of the touch; this would protect against the possibility of unintended "selections" resulting from inadvertently long touches that were intended only to "stop" the scrolling.

In contrast to stationary touching in step **108**, if the system senses motion of the finger touch on the screen, the method reverts to step **104**, again converting the speed and direction of motion of the touch into scrolling motion of the displayed data and restarting the scrolling process. As before, step **104** then proceeds directly into step **106**.

In the embodiment of the system of this invention illustrated in FIG. **2**, the system is shown to comprise a simple personal computer apparatus having a display screen **10**, a central processing unit **12** and a keyboard **14** for inputting manual instruction to the processing unit **12**. In accordance with convention, it will be understood that processing unit **12** includes an internal electronic memory unit (not shown) of conventional design and capabilities. Accordingly, for the purposes of this disclosure, the internal memory unit may be assumed to be the source of a scrollable data display capable of appearing on display screen **10** which is accessible to a hand or stylus device, here stylistically represented by the outline of a hand **16**.

In use, the computer is set up in well-known manner to display the scrollable data on screen **10**, and a hand/finger or stylus **16** is touched to the screen and moved down along the screen to impart an initial downward "scrolling" motion to the data display. Software in the computer interactively responds to the contact with the screen to create the desired displacement motion of the display and the internal timer facility now inherent in such computer apparatus, in cooperation with the programming of processing unit **12** responds to the start of motion by gradually decreasing the speed of displacement, as explained previously herein. When a desired point in the display is seen or approached, the user may apply a hand or stylus **16** to the screen to terminate the scrolling motion. Because the scrolling motion does not involve any moving parts with real or simulated mass, it is possible to stop the motion of the display instantly, without any difficulty or concern for inertial force consequences.

Accordingly, it will now be understood that the system and method of this invention facilitates a rapid, convenient and natural-feeling approach to accessing a scroll-like display of data on a computer screen.

In the embodiment represented in FIG. **3**, the system of this invention is shown to comprise the essential elements of the computer apparatus of FIG. **2** without having the configuration of a computer. That is, the basic components of the system of this invention are here shown to comprise a microprocessor **42** which is in turn coupled to a keyboard **44**, a timer means **43** and a display screen **40**. Each of these components functions in the same manner as its counterparts in the embodiment of FIG. **2**, with microprocessor **42** and the associated timer means **43** together, here serving the same function as central processing unit **12** in FIG. **2**.

Although a preferred embodiment of the invention has been illustrated and described, those having skill in this art will recognize that various other forms and embodiments now may be visualized readily without departing significantly from the spirit and scope of the invention disclosed herein and set forth in the accompanying claims.

The invention claimed is:

1. An improved touch-screen image scrolling system, comprising:

an electronic image display screen;

a microprocessor coupled to said display screen to display information thereon and to receive interactive signals therefrom;

timer means associated with said microprocessor to provide timing capacity therefor;

a source of scroll format data capable of display on said display screen;

finger touch program instructions associated with said microprocessor for sensing the speed, direction and time duration of a finger touch contact with said display screen:

scrolling motion program instructions associated with said microprocessor responsive to said duration of said finger touch contact such that, when said duration exceeds a first given preset minimum time and is accompanied by motion along the surface of said screen followed by separation of said finger touch from said screen, a scroll format display on said screen is caused to begin to scroll in said sensed direction and at said sensed initial speed;

time decay program instructions associated with said microprocessor for reducing the rate of scrolling displacement on said display screen at a given rate until motion is terminated;

stopping motion program instructions associated with said microprocessor for terminating scrolling displacement of the image on said screen upon first occurrence of any signal in the group of signals comprising:

(a) a substantially stationary finger touch on the screen enduring for a period

longer than a preset minimum time, and

(b) an end-of-scroll signal received from said scroll format data source.

2. The improved touch-screen image scrolling system of claim **1**, wherein said scrolling motion program instructions further comprise instructions to move said display in correspondence with movement of the finger touch, in response to movement following a touch having a stationary duration greater than said first preset given minimum time and less than a second given preset minimum time.

3. The improved touch-screen image scrolling system of claim **1**, wherein said scrolling motion program instructions further comprise instructions to move a touch-selected item relative to the stationary display in correspondence with movement of said finger touch, in response to motion following a touch having a stationary duration greater than said second given preset minimum time.

4. The improved touch-screen image scrolling system of claim **1**, wherein

said group of signals for terminating scrolling displacement of the image on said display screen further comprises

(a) a signal indicating that the rate of scrolling displacement on said screen has decayed to a value below a predetermined given value.

5. The improved touch-screen image scrolling system of claim **1**, wherein said microprocessor, and said timer means together comprise a processing unit of a conventional computer.

6. The improved touch-screen image scrolling system of claim **5**, wherein said source of scroll format data capable of display on said display screen comprises part of the memory of said conventional computer.

7. An improved touch-screen image scrolling system, comprising:

an electronic image display screen;

a computer apparatus coupled to said display screen to display information

thereon and to receive interactive signals therefrom;

timer means within said computer apparatus to provide timing capacity therefor;

said computer apparatus having capacity to store scroll format data capable of display on said display screen;

finger touch program instructions associated with said computer apparatus for sensing the speed, direction and time duration of a finger touch contact with said display screen;

scrolling motion program instructions associated with said computer apparatus responsive to said duration of said finger touch contact such that, when said duration exceeds a preset minimum time and is accompanied by motion along the surface of said screen, a scroll format display on said screen is caused to begin to scroll in the sensed direction and at the sensed initial speed;

time decay program instructions associated with said computer apparatus for reducing the rate of scrolling displacement on said display screen at a given rate until motion is terminated;

stopping motion program instructions associated with said computer apparatus for terminating scrolling displacement of the image on said screen upon first occurrence of any signal in the group of signals comprising:

(a) a substantially stationary finger touch on the screen enduring for a period

longer than a preset minimum time, and

(b) an end-of-scroll signal received from said scroll format data source.

8. An improved touch-screen image scrolling system, comprising:

an electronic image display screen;

a microprocessor coupled to said display screen to display information thereon and to receive interactive signals therefrom;

timer means associated with said microprocessor to provide timing capacity therefor;

a source of scroll format data capable of display on said display screen;

finger touch program instructions associated with said microprocessor for sensing the speed, direction and time duration of a finger touch contact with said display screen:

scrolling motion program instructions associated with said microprocessor responsive to said duration of said finger touch contact such that, when said duration exceeds a first given preset minimum time, and is less than a second given preset minimum that is greater than said first minimum, and is accompanied by motion along the surface of said screen, a scroll format display on said screen is caused to begin to scroll in the sensed direction and at the sensed initial speed;

said scrolling motion program instructions further comprising instructions to move a touch-selected item relative to the stationary display in correspondence with movement of the finger touch, in response to motion following a touch having a stationary duration greater than said second given preset minimum time;

said scrolling motion program instructions still further comprising instructions to move said display in correspondence with movement of the finger touch, in response to motion following a touch having a stationary duration greater than said first given preset minimum time and less than said second given preset minimum time;

time decay program instructions associated with said microprocessor for reducing the rate of scrolling displacement on said display screen at a given rate until motion is terminated;

stopping motion program instructions associated with said microprocessor for terminating scrolling displacement of the image on said screen upon first occurrence of any signal in the group of signals comprising:

(a) a substantially stationary finger touch on the screen enduring for a period

longer than a preset minimum time, and

(b) an end-of-scroll signal received from said scroll format data source.

9. The improved method of controlling the scroll-like display of data on an electronic display screen, in accordance with claim **7**, wherein said group of conditions to be sensed for terminating said scrolling motion further comprises: the speed of said scrolling motion on said screen slows to a value below a predetermined given value.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	: 7,184,064 B2	Page 1 of 1
APPLICATION NO.	: 10/736938	
DATED	: February 27, 2007	
INVENTOR(S)	: John Zimmerman and Jacquelyn Annette Martino	

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Insert the following paragraph after the title and before "BACKGROUND OF THE INVENTION":

--This application is a continuation of U.S. Patent Application No. 10/034,375 (now U.S. Patent No. 6,690,387).--

Signed and Sealed this
Fifth Day of April, 2011

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office

4

US007529806B1

(12) United States Patent
Shteyn

(10) **Patent No.: US 7,529,806 B1**
(45) **Date of Patent: *May 5, 2009**

(54) **PARTITIONING OF MP3 CONTENT FILE FOR EMULATING STREAMING**

(75) Inventor: **Yevgeniy Eugene Shteyn**, Cupertino, CA (US)

(73) Assignee: **Koninklijke Philips Electronics N.V.**, Eindhoven (NL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/433,257**

(22) Filed: **Nov. 4, 1999**

(51) **Int. Cl.**

G06F 15/16	(2006.01)
H04N 7/173	(2006.01)
H04K 1/00	(2006.01)

(52) **U.S. Cl.** **709/217**; 709/231; 709/203; 725/114; 705/50

(58) **Field of Classification Search** 709/217–219, 709/231–234, 227; 725/90–100, 112; 345/718; 455/418
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,371,532	A	*	12/1994	Gelman et al.	725/100
5,442,390	A	*	8/1995	Hooper et al.	360/32
5,751,968	A	*	5/1998	Cohen	709/201
5,890,172	A	*	3/1999	Borman et al.	715/501.1
6,005,563	A	*	12/1999	White et al.	345/718
6,012,098	A	*	1/2000	Bayeh et al.	709/246
6,199,076	B1	*	3/2001	Logan et al.	715/501.1
6,263,371	B1	*	7/2001	Geagan et al.	709/231
6,311,058	B1	*	10/2001	Wecker et al.	455/418
6,356,933	B2	*	3/2002	Mitchell et al.	709/203
6,405,256	B1	*	6/2002	Lin et al.	709/231
6,449,638	B1	*	9/2002	Wecker et al.	709/217
6,493,758	B1	*	12/2002	McLain	709/227

FOREIGN PATENT DOCUMENTS

EP	0923033 A1	6/1999

OTHER PUBLICATIONS

Marc Girardot, et al. "Efficient Representation and Streaming of XML content over the Internet Medium", IEEE Conference on Multimedia and Expo., pp. 67-70, 2000.*
"RealNetworks Streaming Media Leadership" article on the web at: http://www.real.com/company/pressroom/rnleadership/index.html.
"Download tunes to a walkman" article on the web at: http://cnn.com/TECH/computing/9909/28/walkman.tunes.idg/index.html.
Java 2 platform API specification, "java.io Class SequenceInputStream" at http://java.sun.com/products/jdk/1.2/docs/api/java/io/SequenceInputStreams.html.

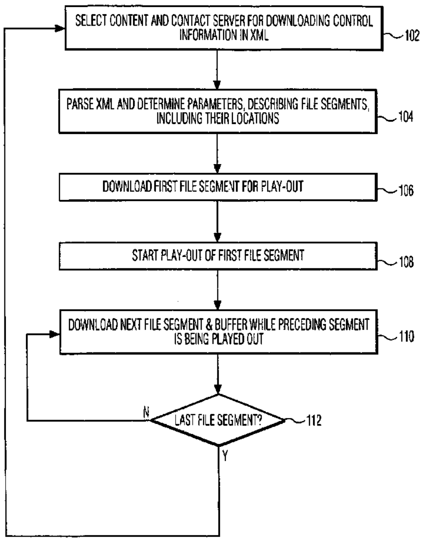
(Continued)

Primary Examiner—Wen-Tai Lin

(57) **ABSTRACT**

An electronic file, e.g., an MP3 file, is partitioned into a sequence of segments at the server side. The first segment is played out upon downloading. While the first segment is being played out, the second is being downloaded and buffered so that it is available when the play out of the first segment is completed. While playing out a current one of the segments, next one(s) of the segments are being downloaded and buffered. This partitioning and sequential play out enables to emulate streaming of a file and to minimize latency while downloading an electronic file.

16 Claims, 2 Drawing Sheets


SELECT CONTENT AND CONTACT SERVER FOR DOWNLOADING CONTROL INFORMATION IN XML
102
PARSE XML AND DETERMINE PARAMETERS, DESCRIBING FILE SEGMENTS, INCLUDING THEIR LOCATIONS
104
DOWNLOAD FIRST FILE SEGMENT FOR PLAY-OUT
106
START PLAY-OUT OF FIRST FILE SEGMENT
108
DOWNLOAD NEXT FILE SEGMENT & BUFFER WHILE PRECEDING SEGMENT IS BEING PLAYED OUT
110
N
LAST FILE SEGMENT?
112
Y

OTHER PUBLICATIONS

Java 2 platform API specification, “java.io Class InputStream” at http://java.sun.com/products/jdk/1.2/docs/api/java/io/InputStreams.html.

Java 2 platform API specification, “Interface Enumeration” at http://java.sun.com/products/jdk/1.2/docs/api/java/io/FileInputStreams.html.

Java 2 platform API specification, “java.io Class FileInputStreams” at http://java.sun.com/products/jdk/1.2/docs/api/java/util/Enumeration.html.

Java 2 platform API specification, Java (TM) 2 Platform, Standard Edition, v1.2.2 API Specification on the Web at http://java.sun.com/products/jdk/1.2/docs/api/overview__summary.html.

“Efficient Representation and Streaming of XML Content Over the Internet Medium” XP002160596, 2000 IEEE Conf. On Multimedia and Expo.

* cited by examiner

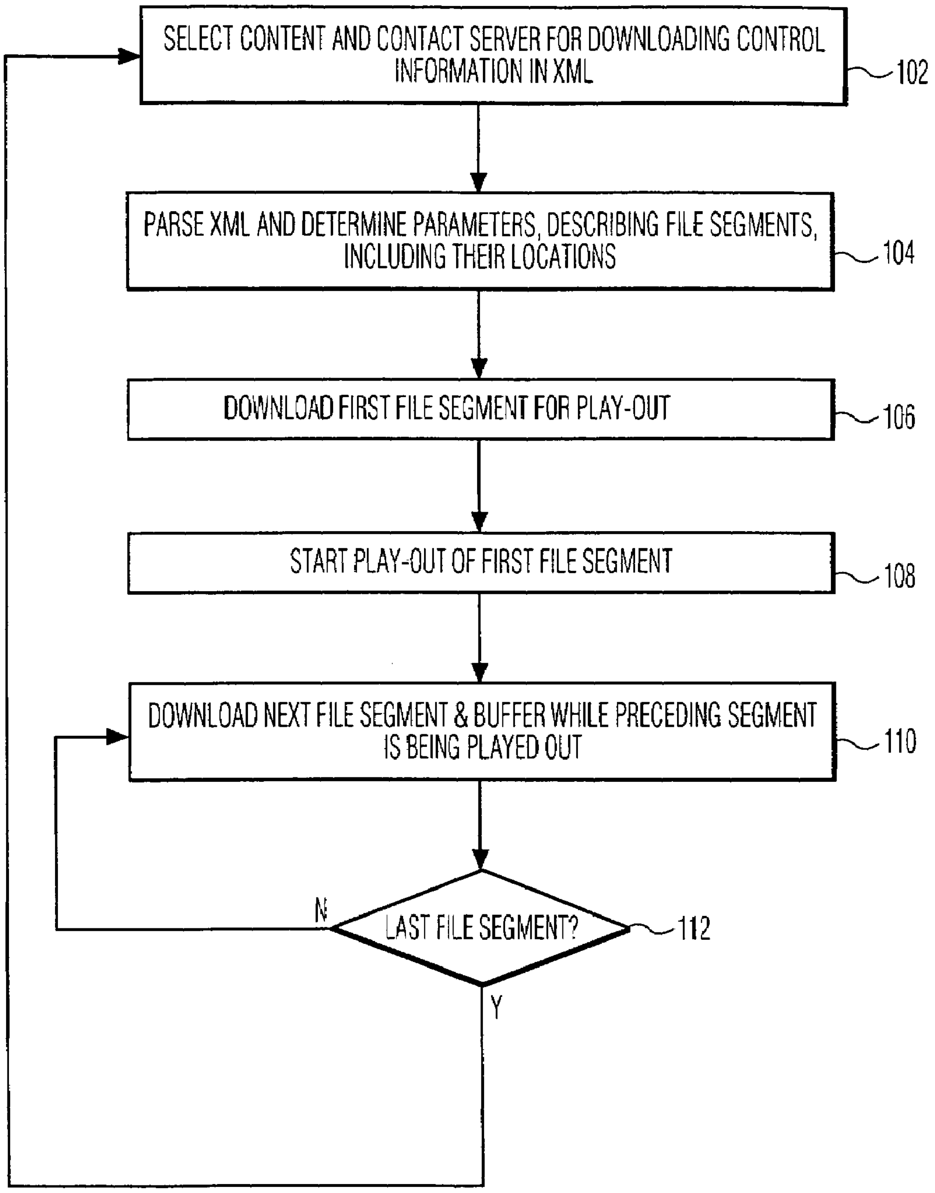
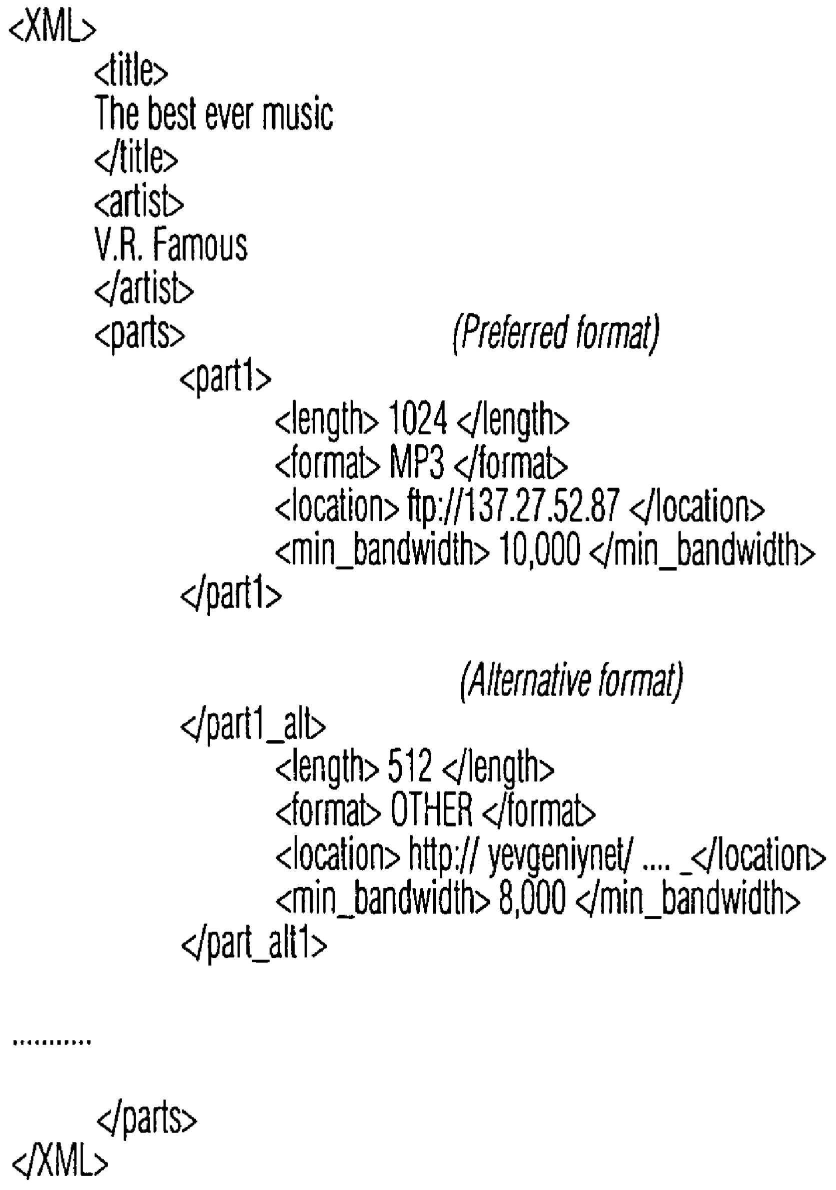

SELECT CONTENT AND CONTACT SERVER FOR DOWNLOADING CONTROL INFORMATION IN XML
102
PARSE XML AND DETERMINE PARAMETERS, DESCRIBING FILE SEGMENTS, INCLUDING THEIR LOCATIONS
104
DOWNLOAD FIRST FILE SEGMENT FOR PLAY-OUT
106
START PLAY-OUT OF FIRST FILE SEGMENT
108
DOWNLOAD NEXT FILE SEGMENT & BUFFER WHILE PRECEDING SEGMENT IS BEING PLAYED OUT
110
N
LAST FILE SEGMENT?
112
Y

FIG. 1



```
<XML>
        <title>
        The best ever music
        </title>
        <artist>
        V.R. Famous
        </artist>
        <parts>                            (Preferred format)
                <part1>
                        <length> 1024 </length>
                        <format> MP3 </format>
                        <location> ftp://137.27.52.87 </location>
                        <min_bandwidth> 10,000 </min_bandwidth>
                </part1>

                                            (Alternative format)
                </part1_alt>
                        <length> 512 </length>
                        <format> OTHER </format>
                        <location> http:// yevgeniynet/ .... _</location>
                        <min_bandwidth> 8,000 </min_bandwidth>
                </part_alt1>

...........

        </parts>
</XML>
```

FIG. 2

PARTITIONING OF MP3 CONTENT FILE FOR EMULATING STREAMING

FIELD OF THE INVENTION

The invention relates to content and/or control communications between multiple computer systems, or to such communications between computer systems and consumer devices. Specifically, the invention relates to communication constrained by bandwidth or limited by data processing resources available to the receiving system or device, especially if the communications are received by the user in real time. The type of communications can be, e.g., broadcast, multi-cast or point-to-point.

BACKGROUND ART

Consider current major technologies for delivering digital content, such as audio, video, etc. The streaming method for audio, e.g., RealAudio by RealNetworks, consists of playing-out audio at a client device, while constantly sending data from the server to the client. The technology provided by RealNetworks comprises an encoder, a server, a splitter/cache and a player system with two-way intelligence to resolve network congestion, lost packet conditions and negotiate complex internet protocols. More specifically, the known technology comprises an automatic, variable bit-rate encoding and delivery system for audio and video. The system scales to megabit connection rates and dynamically adjust the transmission rate as delivery rate varies due to network congestion. The format and the encoding/decoding methods of the data are proprietary. The server and the client synchronize receiving and playing in a way pre-defined by the particular architecture. The communication stack software is tightly coupled to the interpretation layer (application and user interface (UI)). Manufacturers of such technology promote high level of integration between client and server software, as a complete vertical solution. This approach mostly excludes third parties from developing custom server software (e.g., advertizing, services) and/or client applications (UI, special effects, etc.).

Another known method is downloading of a content file from a remote computer with subsequent play-out on the client. MP3 is a widely known audio data format used within the downloading context. There are other data formats, e.g., MP4 for video data etc. The major advantage of the above mentioned method is its open data standard approach. As long as the right format of the content file is observed during encoding, client and server software/hardware manufacturers are free to develop their own solutions/products.

A major problem with the complete download approach is the inherent latency: there is a delay between the beginning of the download and the start of the play-out. The larger the file and or smaller the communication bandwidth, the longer it takes to transfer the content from the server to the client. This is particularly undesirable in consumer electronics systems, where perceived delay is detrimental to market acceptance of an open architecture.

SUMMARY OF THE INVENTION

It is an object of the invention to provide an open architecture solution for content delivery in a download approach that allows for a low or negligible play-out latency.

To this end the content file is split into multiple parts. Each part or segment requires a relatively short download time. Therefore, the play-out latency is determined by the download time of the first part. The size of the individual part can be determined by the communications bandwidth, e.g., through pinging for a latency-check. The client device/application receives control information about the content. This control information comprises, for example, information relating to the size and memory location of the whole file as well as of it parts at the server. If the client is not capable of processing split data, it proceeds with the traditional approach, i.e., downloads the whole file and then plays it out. In case the client is capable of processing parts of the content, it uses the relevant control information about the parts in order to continue downloading data, while playing. Data play-out, also called "rendering", is computation-intensive, since it requires a plurality of decoding operations. Data download is bandwidth-intensive. Accordingly, simultaneous play-out and downloading do not significantly compete for the same system resources. This separation between downloading and processing can be efficiently used in a multi-process and/or multi-thread environment.

Preferably, the information contains references to the file location as well as references to the locations of the parts. The intended bandwidth information is associated with the parts. The client may make its own decisions regarding how many parts to download before the start of the play out (execution).

The parts can have different data formats. The format of some of the parts can be proprietary. Information about alternative content parts, regarding bandwidth, format, location access options, etc., can be provided. Content parts can physically reside on different servers. Content can be split into parts consistent within the semantics of the content, e.g., end of musical phrase, paragraph, target control device, etc. A third party may insert its own content parts in between the original content parts. The third party parts contain, for example, advertisements, commentary, customization options. The format of parts for play-out may be chosen according to user-related information, e.g., personal preferences, level of access to premium services, quality of the equipment, bandwidth sharing/fluctuation conditions, etc.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail and by way of example with reference to the accompanying drawing wherein:

FIG. **1** is a flow diagram illustrating the various steps in a method according to the invention; and

FIG. **2** gives an example of control code.

Throughout the Figures, same reference labels indicate similar or corresponding features.

PREFERRED EMBODIMENTS

The invention enables emulating the streaming of files while using a download approach. FIG. **1** illustrates a flow diagram **100** with various steps involved in the playing-out of a segmented file at the client.

In step **102**, the client contacts the server selects the particular content file and downloads the control information that enables the retrieving and playing out of the segmented file. The control information describes the locations, e.g., URL's, and size of the various file segments, and provides, e.g., UI functionalities at the client. In this example, the control information is coded in XML.

In step **104** the XML code is parsed. Parsing of XML is well known in the art. A person skilled in the art can download an XML interpreter, including source code, from the Internet, see e.g. www.ibm.com/xml. Thus, the client is enabled to get information about the content information and the URLs of the first and subsequent file segments.

In step **106**, the first file segment is downloaded for play-out. Communicating with a remote server is a well known technology. For example, Java 2.0 provides a set of standard classes that enable retrieving a remote file into a buffer or as a stream.

In step **108**, the rendering of the first segment is started. The buffered content of the first segment is forwarded to a decoding/playing module. The decoding/playing module decodes the file format, e.g., MP3. The playing of the supplied stream of bits involves a number of standard operating system calls to its drivers a technique well known in the art.

In step **110**, the next file segment is downloaded at the client and stored in a buffer while the previous file segment, here the first file segment, is being played out. One option is to have the downloaded files buffered in a sequence or linked list of buffers. This functionality is typically provided by the operating system of the client. For example, MS Windows family of products creates a memory buffer associated with the file every time an API call opens the file. Alternatively, in a thread- and/or process-rich environment, several threads and/or processes can be organized to independently retrieve file segments, while playing out the content of other segments. Working with threads is a skill common for software engineers. For example, Java 2.0 from Sun Microsystems provides classes supporting multiple threads. Similarly, Microsoft SDK for the Windows family of products makes thread- or process-related functionalities available to programmers.

Upon completion of playing out the first segment, the second segment is passed on from the buffer to the decoding/playing module. This can be implemented by means of, e.g., a linked list. As known, a linked list is a data structure wherein each element (here: segment) has content data and a pointer to a next element (here: next segment).

The decoding/playing module has to decode the file format. The decoding program represents a standard task to a person skilled in the art to program a decoding procedure according to a widely published standard (MP3, etc.). The playing of the supplied stream of bits involves a number of standard operating system calls to its drivers—a technique well known in the art.

FIG. **2** gives an example of information-describing content coded in XML. The code fragment labels the segments as having a title "The best ever music" performed by "V. R. Famous" and having several parts. The segment labeled "part**1**" is in a preferred format and described the length of the part, e.g., in bytes, the format, the minimum bandwidth required for a connection, and the location on the Internet. An alternative first part is labeled "part**1** alt" having a different length, different format, different minimum bandwidth requirement, and a different location. The XML code can be combined with XSL for generating a user level UI at the user's client. The client thus can automatically choose the format compatible with the client's play-out capabilities.

When the client has selected the proper file, either the one of which the first part is represented here as in the preferred format or the one in the alternative format, the content of the first part is downloaded from the location specified and playing out is started automatically under application control. Combining multiple sequenced inputs is well understood in the industry. For example, Java JDK v.1.2 from Sun Microsystems, Inc. provides a class java.io.SequenceInputStream as a standard component of the io class library. SequenceInputStream represents the logical concatenation of other input streams. It starts out with an ordered collection of input streams and reads from the first one until end of file is reached, whereupon it reads from the second one, and so on, until end of file is reached on the last of the contained input streams. An object of the java.io.SequenceInputStream class can be initialized by, e.g., enumeration of objects of the InputStream class. This abstract class is the superclass of all classes representing an input stream of bytes, including the class FileInputStream. In case of the downloading of multiple file parts, an application can create instances of the FileInputStream class from local temporary files into which the parts are being downloaded. The contents of those multiple local files will be supplied to the Sequencer. The rendering component of the application will read the information out it as if it were just a single local file.

The segmentation of the content file into separately downloadable segments enables a third party, such as a service provider, to insert between two segments specific content information, e.g., advertisements to be rendered on the client's display.

During operation, the client application could select a next segment in a different format for the same content to adapt to changing circumstances, e.g., lower bandwidth due to network congestion. Also, the user could be prompted to subscribe to a service that as a demo lets the user download only the first segment in a high quality and the next segments in a lower quality. The combination of XML and a corresponding parser and interpreter at the client controls the downloading and playing out as explained above. Accordingly, the client pulls the content segments from the locations indicated in the XML control information for buffering and subsequent play-out.

The implementation of a client in this client-server architecture can be done in a variety of ways. A first example is a hardware-based single-purpose device, similar to the Rio MP3 player by the Diamond Corp. In order to accommodate the method of the invention, the player needs, in addition, an XML parser, the ability to interpret XML and the ability to download and play-out content segments sequentially. A second example is to implement the method of the invention as a software application on a multi-purpose computing device, e.g., a PC or a set top box. The device has the software implementing the functionalities mentioned above. In a graphics-rich environment, multiple GUI's are represented to the user for further customization.

The following co-pending applications are incorporated herein by reference:

U.S. Ser. No. 09/406,642 filed Sep. 27, 1999 for Raoul Mallart for SCALABLE SYSTEM FOR VIDEO-ON-DEMAND. This patent document relates to a Video-on-Demand service (VOD) that is emulated in a Near-Video-on-Demand (NVOD) architecture. Content information is made available to an end-user in the NVOD architecture. An introductory portion of the content information is stored at the end-user's equipment, e.g., by downloading overnight. During playing out of the introductory portion at the end-user enabling the content information supplied in the NVOD architecture is buffered at the end-user's equipment. The equipment is controlled to switch from playing out the introductory portion stored to playing out the buffered content information.

U.S. Ser. No. 09/189,534 filed Nov. 10, 1998 for Eugene Shteyn for CONTENT SUPPLIED AS SOFTWARE OBJECTS FOR COPYRIGHT PROTECTION. This document relates to supplying content information such as a movie, an audio file or a textual message to an end-user in a software object. The object has an encapsulated procedure for end-user access of the content information in a runtime environment. The object can specify time frame for and manner wherein the content information is to be accessed. Since the procedure is encapsulated in the object together with the content data, and since transport of the object over the Internet is done after serializing, an adequate degree of security is provided against unauthorized play-out or copying.

U.S. Ser. No. 09/149,950 filed Sep. 9, 1998 for Raoul Mallart for REAL TIME VIDEO GAME USES EMULATION OF STREAMING OVER THE INTERNET IN A BROADCAST EVENT. This patent document relates to emulating streaming of animation data over the Internet to a large number of clients in a broadcast application on a client-server network. The animation is considered a sequence of states. State information is sent to the clients instead of the graphics data itself. The clients generate the animation data itself under control of the state information. The server and clients communicate using a shared object protocol. Thus, streaming is accomplished as well as a broadcast without running into severe network bandwidth problems. This is approach is used to map a real life event, e.g., a motor race, onto a virtual environment in order to let the user participate in a virtual race against the real life professionals, the dynamics of the virtual environment being determined by the state changes sent to the user.

U.S. Ser. No. 09/138,782 filed Aug. 24, 1998 for Raoul Mallart and Atul Sinha for EMULATION OF STREAMING OVER THE INTERNET IN A BROADCAST APPLICATION. In a broadcast application on a client-server network the streaming is emulated of animation data over the Internet to a large number of clients. The animation is considered a sequence of states. State information is sent to the clients instead of the graphics data itself. The clients generate the animation data itself under control of the state information. The server and clients communicate using a shared object protocol. Thus, streaming is accomplished as well as a broadcast without running into severe network bandwidth problems.

U.S. Ser. No. 09/283,545 filed Apr. 1, 1999 for Eugene Shteyn for TIME- AND LOCATION-DRIVEN PERSONALIZED TV. This document relates to a service for personalized video recorders such as the one from TiVo-Philips. The recorder has a hard-disk that serves as a random-access buffer.

I claim:

1. A method of, at a client device, forming a media presentation from multiple related files, including a control information file, stored on one or more server computers within a computer network, the method comprising acts of:

- downloading the control information file to the client device;
- the client device parsing the control information file; and
- based on parsing of the control information file, the client device:
- identifying multiple alternative flies corresponding to a given segment of the media presentation,
- determining which files of the multiple alternative files to retrieve based on system restraints;
- retrieving the determined file of the multiple alternative files to begin a media presentation, wherein if the determined file is one of a plurality of files required for the media presentation, the method further comprises acts of:
- concurrent with the media presentation, retrieving a next file; and
- using content of the next file to continue the media presentation.

2. The method of claim **1**, wherein partitioning of media presentation information between the multiple related files is determined by information about the client.

3. The method of claim **1**, wherein partitioning of media presentation information between the multiple related files is determined by information about the computer network.

4. The method of claim **1**, wherein the media presentation comprises an audio presentation.

5. The method of claim **1**, wherein the media presentation comprises a video presentation.

6. The method of claim **1**, wherein partitioning of media presentation information between the multiple related files is described within the control information file using tags corresponding to respective files.

7. The method of claim **1** wherein the control information file is an XML file.

8. The method of claim **7**, wherein the XML file identifies the multiple alternative files corresponding to the given segment of the media presentation, further comprising an act of partitioning the media presentation into multiple MP3 files corresponding to a portion of the multiple alternative files.

9. A method of storing media presentation information within a computer network including multiple server computers, the method comprising acts of:

- storing on a server computer a control information file of a format to be parsed by a client device; and
- storing on one or more server computers multiple alternative files corresponding to a given segment of a media presentation accessible by the client device to, based on parsing of the control information file, determine which file of the multiple alternative files to retrieve based on system constraints to form a media presentation from the multiple alternative files.

10. The method of claim **9**, wherein the control information file is an XML file.

11. The method of claim **10**, wherein the XML file identifies the multiple alternative files corresponding to the given segment of the media presentation.

12. A client device for forming a media presentation from multiple related files stored on server computers within a computer network, comprising:

- means for downloading files to the client device;
- means for parsing a control information file; and
- means for parsing, based on parsing of the control information file:
- identifying multiple alternative files corresponding to a give segment of the media presentation;
- determining which file of the multiple alternative files to retrieve based on system constraints;
- retrieving the determined file of the multiple alternative files to begin a media presentation, wherein if the determined file is one of a plurality of files required for the media presentation, the means for parsing comprises means for:
- concurrent with the media presentation, retrieving a next file; and
- using content of the next file to continue the media presentation.

13. The device of claim **12**, wherein the control information file is an XML file.

14. The device of claim **13**, wherein the XML file identifies multiple alternative MP3 files corresponding to a portion of the given segment of the media presentation, the means for retrieving comprising means for selecting and retrieving one of the multiple alternative MP3 files.

15. The device of claim **12**, wherein:

the device interprets the control information to retrieve multiple files from the computer network for sequential play-out.

16. The device of claim **15**, wherein:

the means for parsing comprises an XML parser; and

the retrieving and using comprises an XML interpreter.

* * * * *

5

US005910797A

United States Patent [19]

Beuk

[11] **Patent Number: 5,910,797**

[45] **Date of Patent: *Jun. 8, 1999**

[54] **PORTABLE DATA PROCESSING APPARATUS PROVIDED WITH A SCREEN AND A GRAVITATION-CONTROLLED SENSOR FOR SCREEN ORIENTATION**

[75] Inventor: **Leonardus G. M. Beuk**, Eindhoven, Netherlands

[73] Assignee: **U.S. Philips Corporation**, New York, N.Y.

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] Appl. No.: **08/601,140**

[22] Filed: **Feb. 13, 1996**

[30] **Foreign Application Priority Data**

Feb. 13, 1995 [EP] European Pat. Off. 95200338

[51] **Int. Cl.**^{6} **G09G 5/08**

[52] **U.S. Cl.** **345/157**; 345/156; 463/7

[58] **Field of Search** 345/7, 112, 8, 345/145, 156, 157, 161, 163; 463/3, 7, 38; 364/708.1

[56] **References Cited**

U.S. PATENT DOCUMENTS

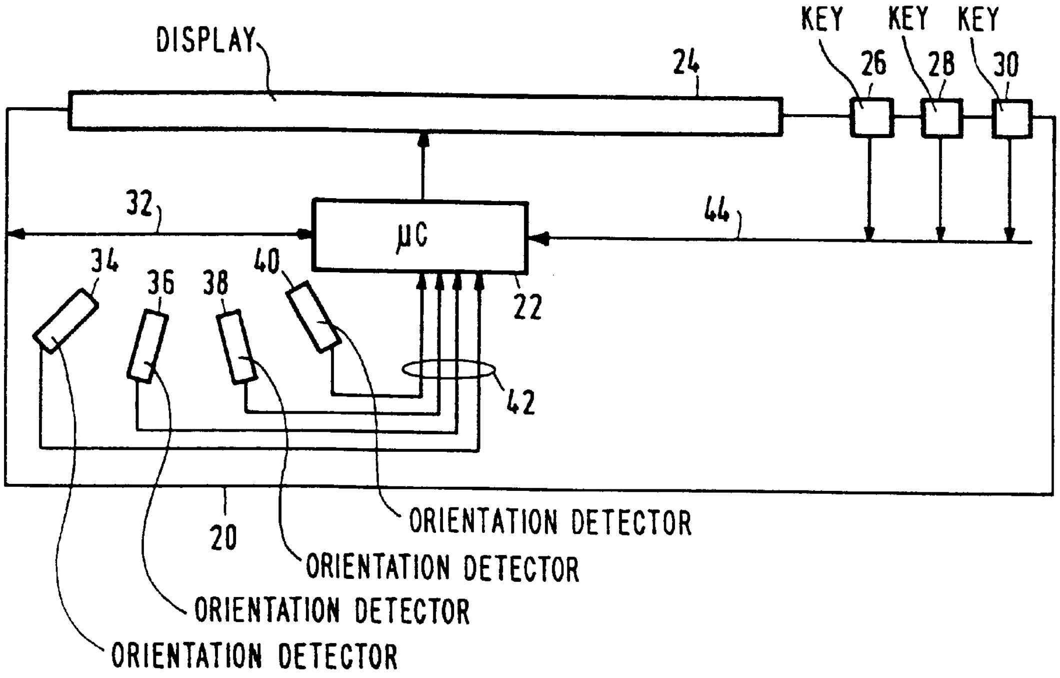
4,503,299	3/1985	Henrard et al.	345/156
5,181,181	1/1993	Glynn	345/163
5,440,326	8/1995	Quinn	345/156
5,526,022	6/1996	Donahue et al.	345/156
5,602,569	2/1997	Kato	345/156

Primary Examiner—Richard A. Hjerpe
Assistant Examiner—Kent Chang
Attorney, Agent, or Firm—Brian J. Wieghaus

[57] **ABSTRACT**

A portable data processing apparatus has an integrated screen that displays one or more graphical or other objects presented thereto. The screen has a gravitation-controlled sensor for measuring a spatial orientation thereof. The apparatus has a programmed data processor for under control of a predetermined range of spatial orientations imparting a non-stationary motion pattern to a predetermined selection among the objects. The motion can be used in the way of a joystick. Eventually it may result in off-screen dumping, loading, or transfer of an associated object.

11 Claims, 2 Drawing Sheets



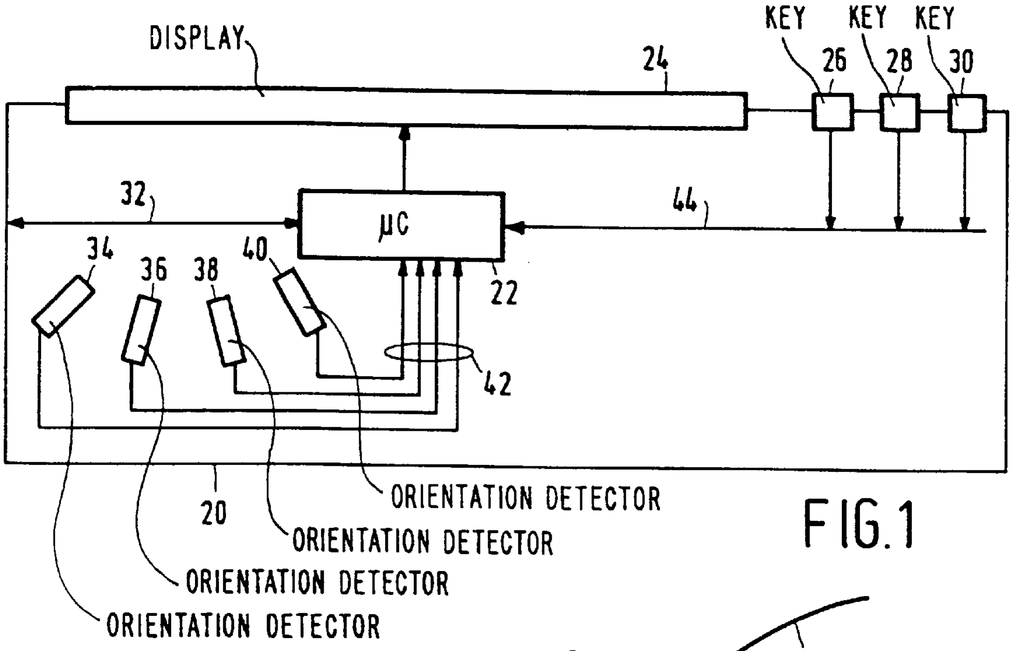


FIG.1

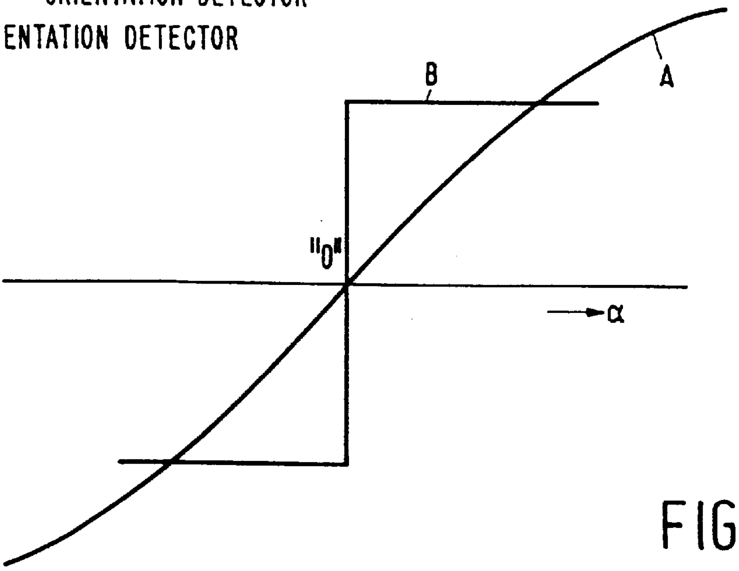


FIG.2

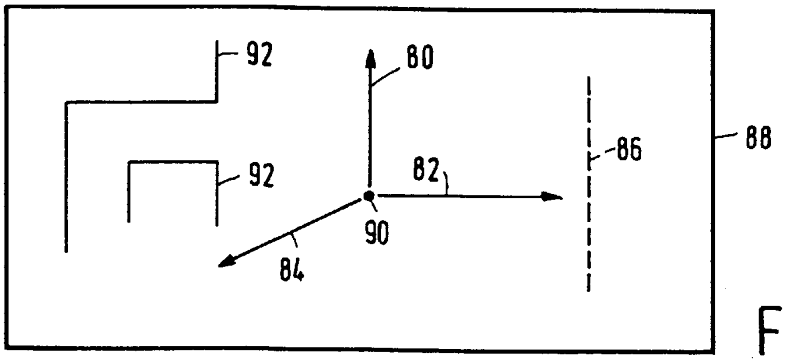


FIG.3

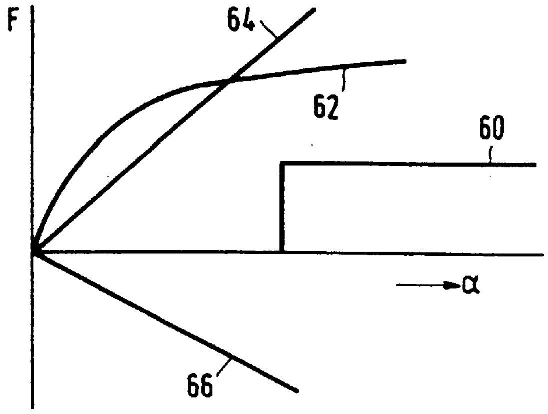

F
64
62
60
α
66

FIG.4

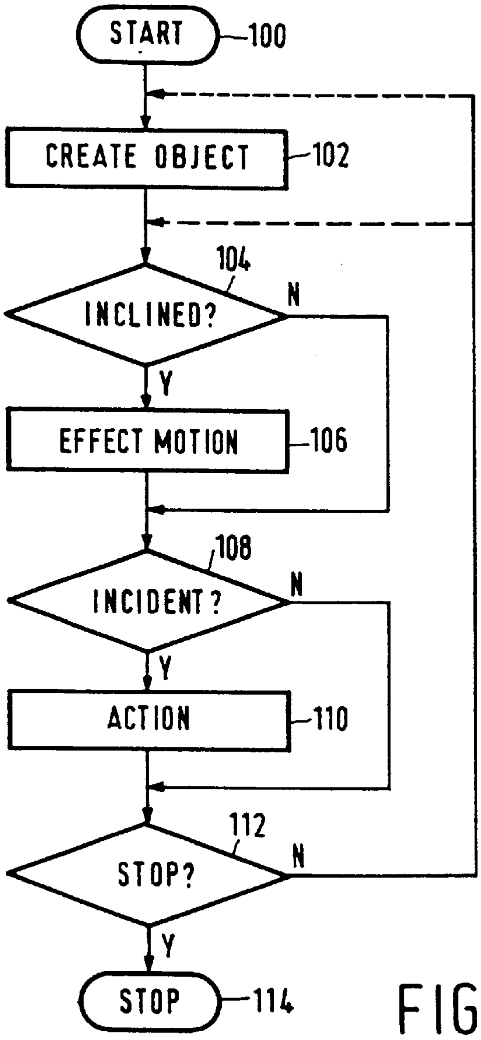

START
100
CREATE OBJECT
102
104
INCLINED?
N
Y
EFFECT MOTION
106
108
INCIDENT?
N
Y
ACTION
110
112
STOP?
N
Y
STOP
114

FIG.5

PORTABLE DATA PROCESSING APPARATUS PROVIDED WITH A SCREEN AND A GRAVITATION-CONTROLLED SENSOR FOR SCREEN ORIENTATION

BACKGROUND OF THE INVENTION

The invention relates to a portable apparatus having data processing means and integrated screen means for displaying one or more graphical or other objects presented by said data processing means, said screen means having gravitation-controlled sensor means feeding said data processing means for measuring a spatial orientation of said screen means. It has been known to sense the spatial orientation of a display apparatus, for example a television monitor, and control the orientation of the image in such a way that the image is always oriented vertically and with the right side up. The inventor has found that various spatial orientations of an apparatus according to the preamble may control associated object motions on the screen, and has envisaged various useful applications of a device that is enhanced in such manner.

SUMMARY OF THE INVENTION

Accordingly, amongst other things, it is an object of the present invention to provide an apparatus according to the preamble wherein the orientation of the screen can be used to control various different types of motion depending on the actual spatial orientation. Now, according to one of its aspects, the invention provides such apparatus, wherein said data processing means have programmed calculating means for under control of a predetermined range of spatial orientations imparting an acceleration based motion pattern to a predetermined selection among said objects. Due to the fact that the motion is acceleration based, the latter can be used to implement various types of game and to exercise handling skills; in various embodiments, the sensor means operate in the manner of a joystick. By itself, joysticks and similar devices are in wide use. The effect of a joystick may be a bidirectional switch in two mutually perpendicular directions. Independent operation thereof selects four directions. Combined operation selects eight directions. The effect may also be an analog control quantity in two mutually perpendicular directions. Combined operation may then select any direction in an XY coordinate system on the screen. This joystick function is in particular effected by the orientation of the screen influencing the motion pattern of the displayed objects. In contradistinction, with respect to the television apparatus, supra, only the stationary orientation of the image, but no motion thereof may vary with the orientation of the apparatus. The invention does not relate to sensing the orientation of the screen by a device that operates the way of a compass in that it would be based on gyroscopic or magnetic principles. The selection of the moving objects may encompass a single one or more displayed objects, or rather all of them.

Advantageously, the motion is linewise and parallel to an inclination vector of said screen means with respect to a vertical direction. The inclination vector is defined as the difference between the vertical direction in the world coordinate system, and the vertical direction with respect to the orientation of the apparatus. In this way, the inclination can emulate some type of artificial gravity that may induce "pseudo falling" of displayed objects. The acceleration based motion can be subject to steady acceleration or other types of behaviour. Often, changing the screen orientation whilst the gravitation vector remains parallel or nearly parallel to the plane of the screen need have no motion controlling effect.

Advantageously, the motion pattern is restrained by one or more further on-screen objects. Such objects, in the form of gates, channels and the like, can then implement a game based on moving an object through a maze, positioning a ball in a shallow potential dip, and many others that require manipulatory skills from a user person.

Advantageously, a predetermined amount represents a transfer of an associated predetermined object between said screen means and a predetermined off-screen device. In this way, inclination of the apparatus may effect data processing effects per se, even apart from the moving around of the object. Storage, printing, reading from a memory chip card, deleting of text, and transmission to a remote data processing device are realizations of this kind of feature. In case of text, vertical motion thereof may be organized to represent scrolling. In the latter case even an ongoing dialog between two apparatuses of the kind described can be maintained.

Further advantageous aspects of the invention are recited in dependent claims.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other aspects and advantages of the invention will be discussed more in detail with reference to preferred embodiments disclosed hereinafter, and more in particular with reference to appended Figures that show:

FIG. **1** shows an apparatus diagram according to the invention;

FIG. **2** shows various sensor characteristics for the invention;

FIG. **3** shows various motion pattern shapes with the invention;

FIG. **4** shows various motion characteristics with the invention;

FIG. **5** shows a flow chart for use with the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

FIG. **1** shows an apparatus diagram according to the invention. The apparatus comprises a housing **20**, data microprocessor **22**, display screen **24**, keys **26**, **28**, **30** that upon actuation provide key data on key bus **44** and output line **32** for connection to an external peripheral device such as printer or an antenna for broadcast output, or an insert for positioning a memory chip card or similar storage-oriented device. Addition of various other peripherals that are common in the art of hand-held games is feasible. The above configuration can operate in a way that has been widely practised for handheld calculators, handheld game-oriented devices, or so-called Personal Digital Assistants. The display may be 5×5 cms, or any other reasonable dimension, and may also be circular or otherwise non-square. It may be based on standard LCD technology. In addition to the above, the apparatus has gravitation-controlled detectors **34**, **36**, **38**, **40** that singly or collectively measure a spatial orientation around an axis that is perpendicular to the plane of the Figure. A similar arrangement may be provided for measuring the spatial orientation around an axis that is horizontal in the plane of the Figure. The technology of the determination may be based on the weight of an element internal to the detector, such as a drop of mercury that does or does not wet a particular electrical contact. Another solution is that the differential weight of another element of the apparatus in various orientations is determined, such as the weight of the display element itself. For example, a first sensor measures gravitation force in a direction perpendicular to the display surface, such as being based on piezoelectricity or strain gauges. Two other such sensors each measure the gravitation force in one of two mutually perpendicular directions within the plane of the display. These three measured quantities together yield the overall spatial orientation of the apparatus with respect to the direction of gravity. In the latter case, facility could as well be provided for measuring dynamical changes of the spatial orientation, such as by acceleration of the screen. This feature can have an on-off character or an analog representation.

FIG. **2** shows various sensor characteristics for use with the invention. Generally, there are two distinct classes of response as a function of the inclination angle α. Curve A gives an analog or gradual response: for α equal to zero, a standard value is produced, such as "zero". In first approximation, the change of the signal is proportional to the inclination angle. For greater inclination a saturation effect, such as according to a sine curve may occur. Curve B gives a step response: depending on whether the inclination is positive or negative, the signal may have a first or rather a second value. These two values may lie symmetrically with respect to zero. Combining two or more sensors with different orientations may produce orientation values in a wider range of orientations around a single axis, such as by the four sensors in FIG. **1**. Likewise, combination of various sensors may yield orientation in three-dimensional space, again through A/D conversion and trigonometric calculations. Alternatively, the sensor signal may be used directly to control the motion of on screen objects. In the latter case, A/D conversion alone were enough.

FIG. **3** shows various motion pattern shapes realizable with the invention. The display area **88** is rectangular at a size of 8×12 centimetres. The original position of the object is at indication **90**. The object may be a dot as shown, but may have the representation of an fixed-shape icon, or may even be an animated figure of variable shape. It may be a more or less continuous object, such as representing a piece of fluid tar that slowly moves about the screen, while also changing its shape. If non-graphical, it may be a block of text of finite size. The motion may, as shown by arrows **80**, **82**, be restricted to the coordinate directions, or may go in any orientation, as shown by arrow **84**. The motion may be constrained by artificial boundaries such as **86**, or by a part of a maze **92**. If the motion causes touching of the constraint, this may lead to an error signalization, such as in the case of a manipulation game, such as for moving a ball through a maze. The touching then may terminate the game, increase an error score, or cause any well known procedure in this type of games. On the other hand, the touching of the constraint may trigger a distinct operation, such as an output operation on the text block. The outputting of such text block may depend on the direction of motion. For example, if horizontal, the outputting may be effected as a one-shot operation, whereas if vertical, the outputting is by linewise scrolling. If the constraint is nonoperative, the motion may continue to the edge of the screen or even further. The object during motion may rotate and be displayed in the form of a wheel or the like. The motion may be controlled along non-straight trajectories, such as parabolas, or may comprise oscillating or rotary motion or motion components. The motion may be constrained by soft boundaries, such as gravitational potential wells. In all cases, the motion is accelaration based, such as with respect to altering the motion vector of the object with respect to speed or direction; because altering of spatial orientation of the screen effects a dynamical change of the motion pattern.

FIG. **4** shows various motion characteristics realizable with the invention. The horizontal axis gives the inclination angle α as in FIG. **2**. The vertical axis gives a pseudo force exerted on the object. Such a force if steady, in combination with a pseudo mass of the object, would result in a uniform acceleration. Curve **64** gives such a constant force, that would make the object 'fall' under constant acceleration. Curve **66** is directed in the other direction, and would make the object to 'fly like a balloon'. Other characteristics are given by curves **60**, that has a threshold angle, and curve **62**, where the force attains an asymptote. Other characteristics, as well as combinations of the above are feasible. In all cases, the vertical quantity may be the actual velocity attained instead of the force.

FIG. **5** is a flow chart for use with the invention, such as in a manipulatory game. Block **100** represents the start of the game, initializing the score, defining the maze, the level of user person skill, and other game elements as applicable. In block **102**, the object to be moved is created. There may be more than one moving object around that is influenced by the pseudo gravitation, possibly in different ways. In block **104**, the existence of non-zero inclination is sensed, or rather a non-zero change of inclination. If yes, in block **104** the motion is amended; in this example, the motion only depends on actual inclination. If the inclination is steady, the motion remains uniform. In block **108**, occurrence of an incident is detected, such as collision with a constraint. If yes, in block **110** appropriate action is taken, such as bouncing back, increase of error score, termination of the object or of the total game, and the like. Absent the incident, the process goes to block **112**. Here detection of a termination situation is detected. This may relate to power off, to attainment of a limit score for the errors, to attainment of the goal of the game, and so on. If yes, in block **114** the game is terminated. If no in block **112**, the system may revert to block **104** and proceed with the moving object, or rather to block **102**, where a new object is created, and a new round commenced. The game can be extended in many different ways without deviating from the present inventive thought.

What is claimed is:

1. A manipulatable apparatus having data processing means and screen means for displaying one or more graphical or other objects presented by said data processing means, a gravitation-controlled sensor integrated with said screen means and feeding said data processing means for measuring an acceleration of said screen means induced by user manipulation of the screen means, wherein said data processing means have programmed calculating means for under control of a screen motion sensed by said sensing means imparting an acceleration based motion pattern to a predetermined selection among said objects.

2. An apparatus as claimed in claim **1**, wherein said predetermined range of spatial orientations is limited to having a gravitation vector component perpendicular to said screen means.

3. An apparatus as claimed in claims **1**, wherein said gravitation-controlled sensor means control said motion in the manner of a joystick.

4. An apparatus as claimed in claim **1**, wherein said motion is linewise and parallel to an inclination vector of said screen means with respect to a vertical direction.

5. An apparatus as claimed in claim **1**, wherein said motion pattern is different among at least two simultaneous selections among said objects.

6. An apparatus as claimed in claim **1**, wherein said motion is nonuniform in time under control of a static said orientation of the screen means.

7. An apparatus as claimed in claim **1**, wherein said motion pattern is constrained by one or more further on-screen objects.

8. An apparatus as claim **1**, wherein said motion represents a a motion of the object as if the force applied to the screen were applied to the object.

9. An apparatus as claimed in claim **1**, wherein said motion represents a scrolling effect on an associated text object.

10. An apparatus as claimed in claim **1**, wherein a predetermined amount of said motion effects a removal of an associated predetermined object from said screen means and transmission to a remote data processing device.

11. A manipulatable apparatus having data processing means and a display screen for displaying one or more graphical or other objects presented by said data processing means, a gravitation-controlled sensor integrated with said display screen and feeding said data processing means for measuring dynamical changes of the spatial orientation of said display screen induced by user manipulation of the display screen, wherein said data processing means have programmed calculating means for under control of a screen motion sensed by said sensor, due to dynamical changes of the spatial orientation of the screen, imparting an acceleration based motion pattern to a predetermined selection among said objects which motion corresponds to the dynamical change of the spatial orientation of the screen.

* * * * *

6

US006522695B1

(12) **United States Patent**
Bruekers et al.

(10) **Patent No.: US 6,522,695 B1**
(45) **Date of Patent: Feb. 18, 2003**

(54) **TRANSMITTING DEVICE FOR TRANSMITTING A DIGITAL INFORMATION SIGNAL ALTERNATELY IN ENCODED FORM AND NON-ENCODED FORM**

(75) Inventors: **Alphons A. M. L. Bruekers**, Eindhoven (NL); **Johannes M. M. Verbakel**, Eindhoven (NL); **Marcel S. E. Van Nieuwenhoven**, Eindhoven (NL)

(73) Assignee: **Koninklijke Philips Electronics N.V.**, Eindhoven (NL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/270,440**

(22) Filed: **Mar. 16, 1999**

(30) **Foreign Application Priority Data**

Mar. 19, 1998	(EP)	98200870
Dec. 7, 1998	(EP)	98204150

(51) **Int. Cl.**^{7} **H04L 27/00**
(52) **U.S. Cl.** **375/259**
(58) **Field of Search** 375/259, 265, 375/341, 285, 240.24, 240.27; 714/759, 791, 795, 752

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,055,338 A	*	4/2000	Endo et al.	382/247
6,189,123 B1	*	2/2001	Nystrom et al.	714/751
6,304,609 B1	*	10/2001	Stephens et al.	375/259
6,353,613 B1	*	3/2002	Kubota et al.	370/389

OTHER PUBLICATIONS

AES Preprint 4563 "Improved Lossless Coding of 1–Bit Audio Signals" by Fons Bruekers et al, 103rd AES Convention (New York, US).

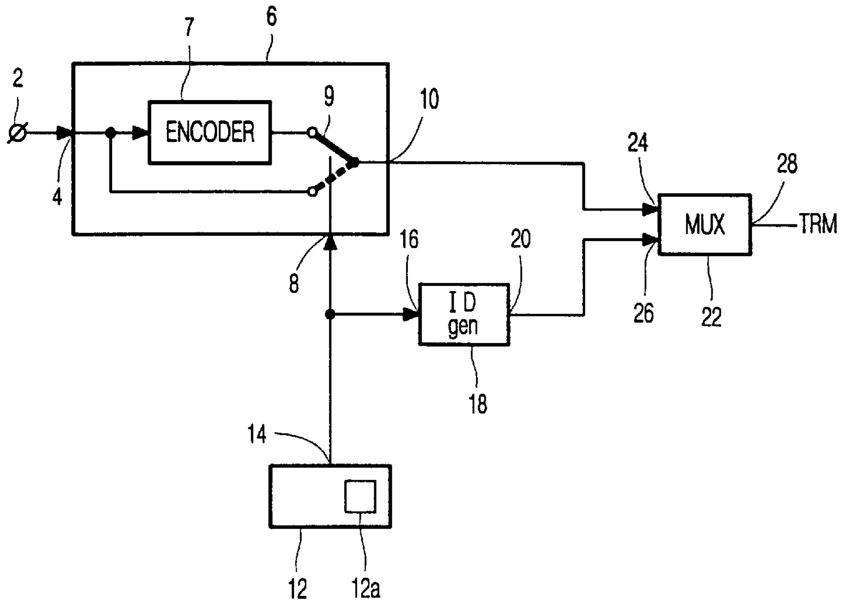
* cited by examiner

Primary Examiner—Chi Pham
Assistant Examiner—Emmanuel Bayard
(74) *Attorney, Agent, or Firm*—Michael E. Belk

(57) **ABSTRACT**

A transmitter transmits a digital information signal via a transmission medium. The digital information signal can be divided into one or more sub-signals. Each sub-signal is transmitted as a non-encoded or as an encoded signal. Thus, the sub-signal is transmitted depending on the compression that can be achieved by the encoder. If the compression is low the sub-signal is transmitted in non-encoded form. For the receiver, an identification is added to the composite signal to be transmitted. A first component of the identification signal indicates if one or more sub-signals are transmitted in encoded form. A second component of the identification signal indicates for each sub-signal, whether it appears in encoded or non-encoded form in the composite signal. The invention provides a composite signal with a minimal number of bits.

18 Claims, 3 Drawing Sheets



A-0042

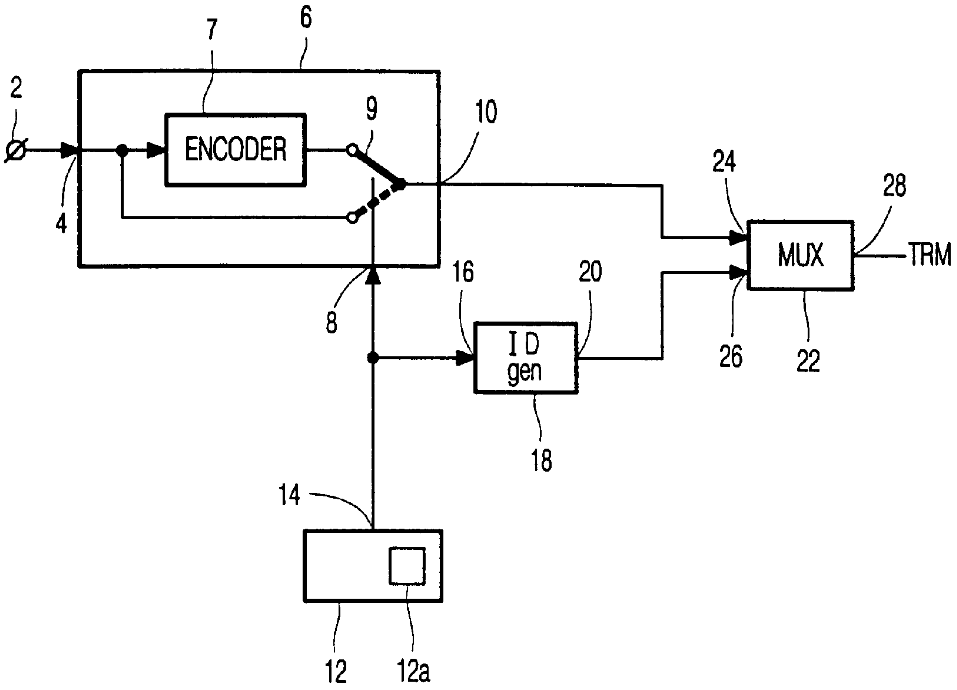

7
6
2
ENCODER
9
10
4
24
28
MUX
TRM
16
20
8
I D
gen
26
22
18
14
12
12a

FIG. 1

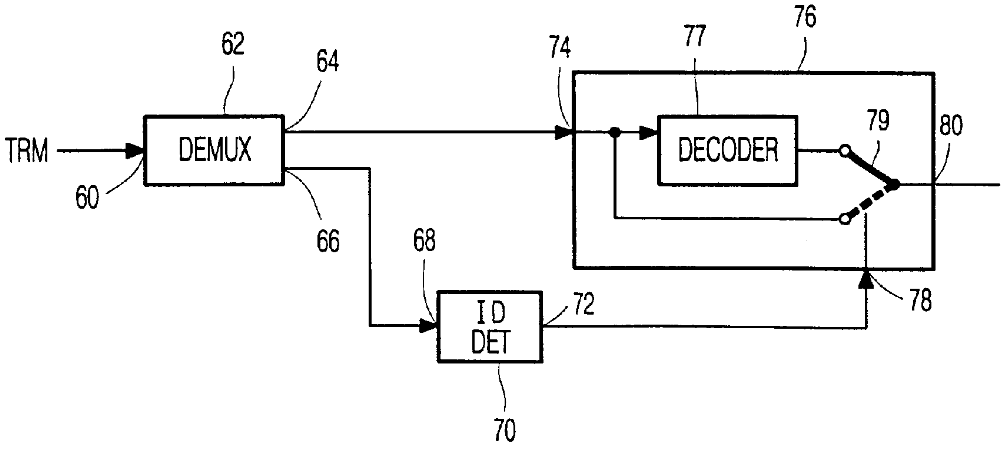

62
64
74
77
76
TRM
DEMUX
DECODER
79
80
60
66
68
I D
DET
72
78
70

FIG. 2

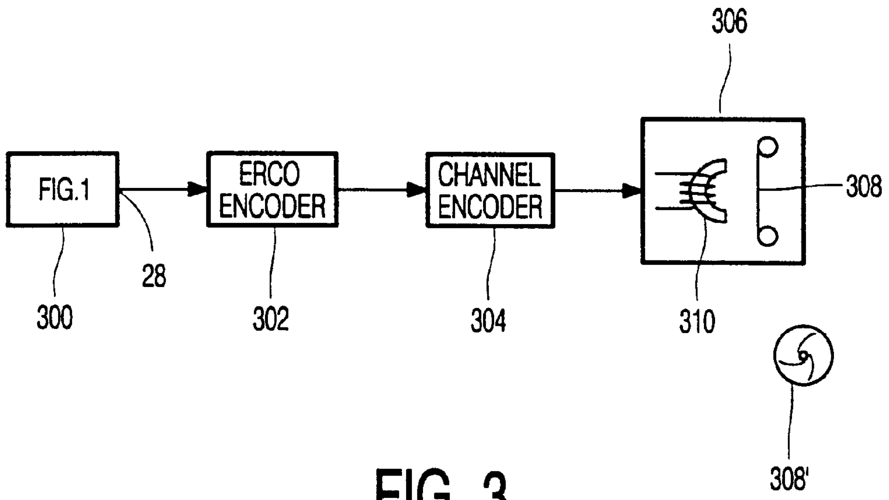

306
FIG.1
ERCO ENCODER
CHANNEL ENCODER
308
300
28
302
304
310
308'

FIG. 3

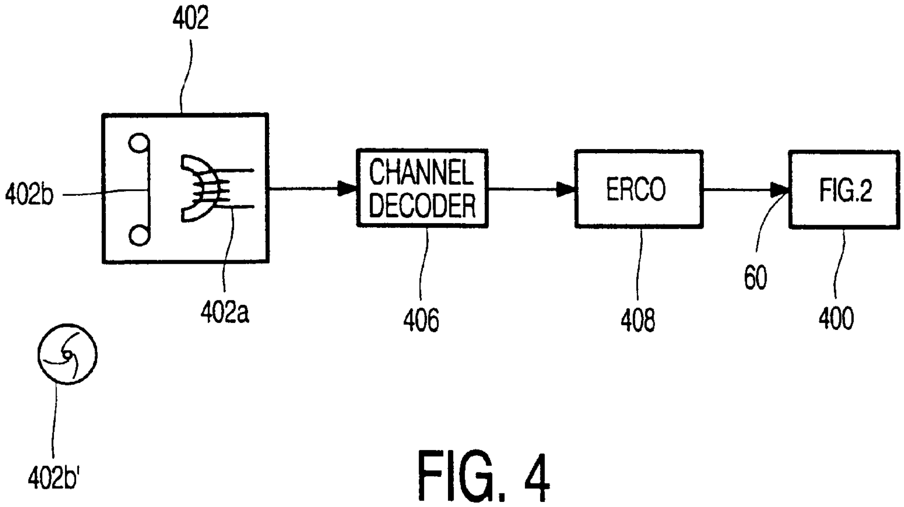

402
402b
CHANNEL DECODER
ERCO
FIG.2
402a
406
408
60
400
402b'

FIG. 4

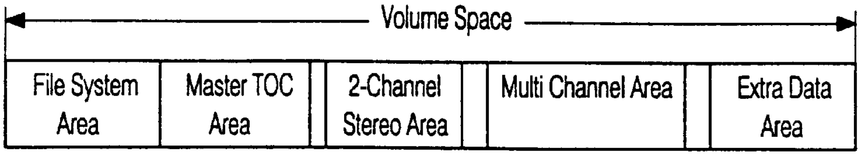


FIG. 5

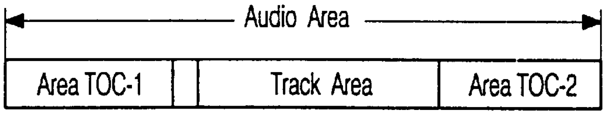


FIG. 6

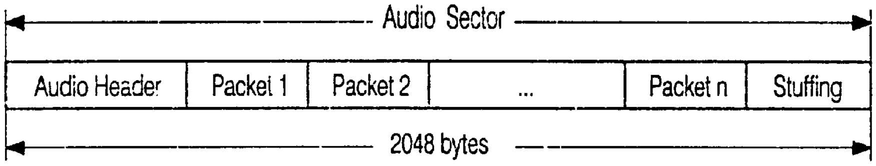


FIG. 7

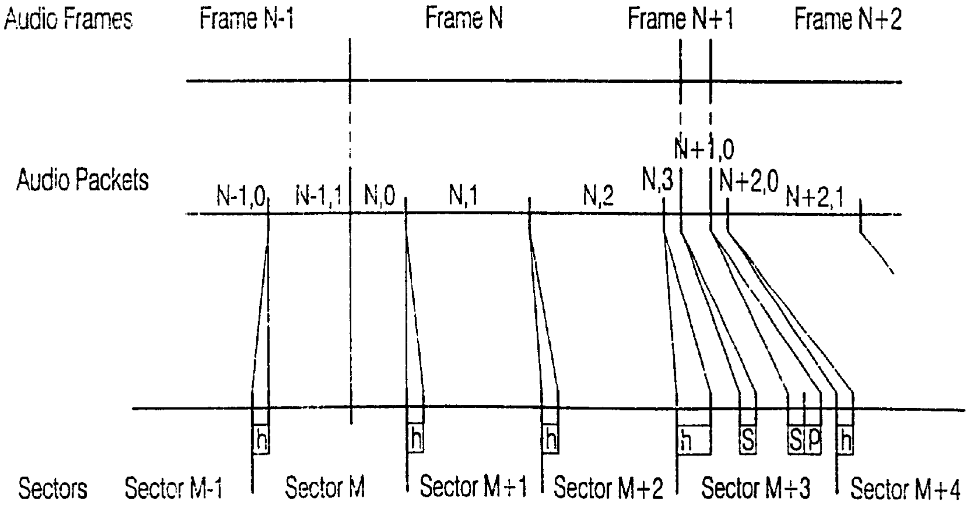


FIG. 8

TRANSMITTING DEVICE FOR TRANSMITTING A DIGITAL INFORMATION SIGNAL ALTERNATELY IN ENCODED FORM AND NON-ENCODED FORM

BACKGROUND OF THE INVENTION

1. Technical Field

The invention is related to the field of signal encoding for compressing the signal and subsequent decoding to reproduce the signal.

2. Related Art

The invention relates to a transmitting device for transmitting a digital information signal via a transmission medium, including:

an input for receiving the digital information signal,

an encoder for encoding the digital information signal and generating an output signal.

The invention further relates to a receiver for receiving a composite signal via a transmission medium, to a method of transmitting a digital information signal via a transmission medium, and to a record carrier carrying a digital information signal having portions which have been or have not been encoded by a given encoding method.

A transmitter and receiver of the type defined in the opening paragraphs is known from the AES preprint 4563 "Improved Lossless Coding of 1-Bit Audio Signals" by Fons Bruekers et al, 103rd AES Convention (New York, US). The known transmitter is intended for efficiently reducing the bit rate for the transmission of a digital information signal. A composite signal thus obtained includes an encoded version of the digital information signal. On an average, the composite signal obtained by the known transmitter contains less bits than a composite signal in which the digital information signal has not been encoded.

SUMMARY OF THE INVENTION

It is an object of the invention to provide a transmitter and/or receiver which transmits a digital information signal with a smaller or at the most equal number of bits. The invention also enables more information to be stored on a record carrier.

To this end, a transmitter in accordance with the invention, further includes:

a controller for generating a control signal to be applied to the encoder, and the encoder generates portions of the output signal in the form of encoded portions of the digital information signal under the influence of a control signal of a first type, and generates portions of the output signal in the form of portions of the digital information signal under the influence of a control signal of a second type;

a first identification signaler for generating a first identification signal of a first type which indicates that the output signal possibly includes a portion of the digital information signal which has been encoded in the encoder, and a first identification signal of a second type which indicates that the output signal does not include any portions of the digital information signal which have been encoded by the encoder;

a second identification signaler for generating, for a portion of the digital information signal, a second identification signal of a first type depending on the control signal of the first type and the first identification signal of the first type, and a second identification

signal of a second type depending on the control signal of the second type and the first identification signal of the first type;

a combiner for combining the output signal of the encoder, the first identification signal and, if the first identification signal is of the first type, the second identification signal so as to obtain a composite signal to be applied to the transmission medium.

In a receiver in accordance with the invention, a demultiplexer derives a first identification signal of a first type and a second type from the composite signal, and decodes a signal portion into a portion of the digital information signal and supplies the portion of the digital information signal depending on a control signal of a first type and supplies signal portion as a portion of the digital information signal in a substantially unmodified form depending on a control signal of a second type, and the receiver further includes:

a controller for generating the control signal for application to the decoder, which controller generates a control signal of the first type depending on the first identification signal of the first type.

A method in accordance with the invention includes the steps of:

generating a control signal;

generating portions of an output signal in the form of encoded portions of the digital information signal under the influence of a control signal of a first type;

generating portions of the output signal in the form of portions of the digital information signal under the influence of a control signal of a second type;

generating a first identification signal of a first type which indicates that the output signal possibly includes a portion of the digital information signal which has been encoded in the encoder, or a first identification signal of a second type which indicates that the output signal does not include any portions of the digital information signal which have been encoded by the encoder;

generating a second identification signal of a first type depending on the control signal of the first type and a first identification signal of the first type;

generating a second identification signal of a second type depending on the control signal of the second type and the first identification signal of the first type;

combining the output signal of the encoder, the first identification signal and, if the first identification signal is of the first type, the second identification signal so as to obtain a composite signal; and

applying the composite signal to the transmission medium.

A record carrier in accordance with the invention carries a digital information signal having portions which have not been encoded and other portions which have been encoded by using a given encoding method, and carries a first identification signal which is of a first type which indicates that the record carrier may carry a portion of the digital information signal encoded using the given encoding method.

The invention is based on recognition of the fact that by using an encoder, the number of bits required to transmit a digital information signal is not always reduced. In the encoder, some signals give rise to an output signal which requires more bits for the representation of the digital information signal than the digital information signal itself. In the device and the method in accordance with the invention, in order to preclude this increase, the representation having the smaller number of bits is transmitted together with an identification signal, which indicates whether or not the signal has been encoded by a given encoding method. A record carrier can store a maximum number of bits. If the record carrier is obtained using the method in accordance with the invention, it can store a composite signal with a larger digital information signal.

BRIEF DESCRIPTION OF THE DRAWING

These and other aspects of the invention will be described in more detail with reference to FIGS. **1** to **8**.

FIG. **1** is a block diagram of a first embodiment of a transmitting device in accordance with the invention.

FIG. **2** is a block diagram of an embodiment of a receiver in accordance with the invention.

FIG. **3** is a block diagram of a transmitter in the form of a recording apparatus.

FIG. **4** is a block diagram of a receiver in the form of a reproducing apparatus.

FIG. **5** shows a structure of a Volume Space on a record carrier.

FIG. **6** shows a structure of an audio Area on a record carrier.

FIG. **7** shows a layout of an Audio Sector on a record carrier.

FIG. **8** shows the relationship between Multiplexed Frames and Audio Sectors.

DETAILED DESCRIPTION OF THE EMBODIMENTS

FIG. **1** is a block diagram of a first embodiment of a transmitter in accordance with the invention. The transmitter has an input terminal **2** for receiving a digital information signal such as a digital audio signal. The digital audio signal may have been obtained by converting an analog version of the digital audio signal into the digital information signal in an analog-to-digital (A/D) converter. The digital information signal may take the form of 1-bit signals, such as a bitstream. It is also possible that the digital information signal received via the input terminal has been obtained using a plurality of pre-processing operations, not shown. The pre-processing operations may include, for example, an encoding method. The digital information signal may include one or a plurality of signal portions. One signal portion of the digital information signal can, for example, be the information recorded in one track on the record carrier, or a group including a number of samples of the digital information signal. The signal portions together constitute the digital information signal. A digital information signal is, for example, all the audio information recorded on a record carrier or a music item which is transmitted via a transmission medium. The input terminal **2** is coupled to an input **4** of encoding unit **6**. The encoding unit **6** includes an encoder **7** to convert the signal received at the input **4** into an encoded signal. The encoder **7** may be a lossless encoder as described in the AES preprint 4563 “Improved Lossless Coding of 1-Bit Audio Signals” by Fons Bruekers et al., 103rd AES Convention (New York, US). Alternatively, the encoder **7** may be a lossy encoder. The encoding unit **6** supplies an output signal to an output **10**. Depending upon a control signal applied to a control input **8**, a switching element **9** couples an output of the encoder **7** or the input **4** to the output **10**, as a result of which, the output signal includes the encoded signal or the signal received at the input **4**.

The encoding unit **6** may also include an encoder **7** which supplies the digital information signal to the output of the encoder in a modified or unmodified form depending on the coefficients used in the encoder. For example, in the Application EP 98200869 (PHN 16.831), not yet published at the time of filing of the present Application, an arithmetic encoder is described, which in the case of a coefficient having the value 0.5, applies the signal received at the input of the arithmetic encoder to the output of the arithmetic encoder in a substantially unmodified form. By the selection of suitable coefficients in the encoder depending on the control signal, the encoder can apply an encoded digital information signal or a substantially unmodified digital information signal to the output. In the case of coefficient controlled encoding, the encoding unit **6** does not include a switching element as shown in FIG. **1**.

The embodiment shown in FIG. **1** also has a controller **12** for applying the control signal to the control input **8** of the encoding unit **6** and to a control input **16** of the identification signaler **18** for deriving an identification signal. The controller **12** may take the form of an input terminal. However, the controller **12** may alternatively include reduction estimator **12***a* to determine the data reduction which is achieved or can be achieved by the conversion of the signal into the encoded signal in the encoder **7**. For example, if an entropy encoder is used in the encoder **7**, it is possible to determine with satisfactory probability the degree of data reduction of the signal caused by encoding with the aid of the statistical distribution of a signal applied to the input of the entropy encoder and/or the probability table used by the entropy encoder. When a prior estimate is made, it is not necessary to wait until the signal has been encoded in order to determine the data reduction. As a result, a digital information signal can be processed and transmitted more rapidly by the transmitter. Reduction estimator **12***a* can determine the data reduction of both the digital information signal and the individual signal portions. Subsequently, the data reduction is compared with a predetermined factor. If encoding leads to a data reduction greater than a predetermined factor, a control signal of the first type is generated. If encoding leads to a data reduction smaller than the predetermined factor, a control signal of the second type is generated.

Identification signaler **18** derives an identification signal depending on the control signal received at the control input **16**. The identification signal is applied to an output **20**. Identification signaler **18** also indicates, in the identification signal, whether the encoding unit **6** supplies a signal to the output **10** of the encoding unit **6** in an encoded form or in a substantially unmodified form. The identification signal includes a first component that indicates that possibly a signal portion of the digital information signal is supplied to the output **10** of the encoding unit **6** in an encoded form. If the identification signal includes this first component, the identification signal also includes a second component, which indicates for each of the signal portions, whether the signal is supplied to the output **10** of the encoding unit **6** in an encoded form or substantially unmodified.

The combiner **22** has a first input **24** coupled to the output **10** of the encoding unit **6**, a second input **26** coupled to the output **20** of the identification signaler **18** for generating the identification signal, and an output **28**. The combiner generates a composite signal from the output signal of the encoding unit **6** and the identification signal. The composite signal is applied to the output **28** in order to be transmitted via a transmission medium (TRM).

The transmitting device as described hereinbefore operates as follows. The digital information signal is applied to the input terminal **2** and is supplied to the encoding unit **6**. The controller **12** applies a control signal to the encoding unit **6**. If the control signal of the first type is received, the output signal of the encoding means contains the encoded signal. If the control signal of the second type is received, the switching element **9** couples the input **4** of the encoding unit **6** to the output **10** of the encoding unit **6**. The output signal of the encoding unit **6** then contains the digital information signal. The control signal can be defined externally. For example, for some types of digital information signals, encoding these digital information signals would lead to an increased number of bits. In such case, the digital information signal would be expanded rather than compressed. This is undesirable, because this expansion may give rise to problems. These problems may be, for example, an inadequate storage capacity or an insufficient bandwidth in order to transmit the digital information signal via the transmission medium. A control signal of the second type is applied when it is known that encoding of the digital information signal does not yield the desired data reduction. In that case, the digital information signal is not applied to the combiner **22** in an encoded form. However, when it is known that encoding leads to a significant data reduction, then a control signal of the first type will be applied. The identification signaler **18** generates the identification signal corresponding to the relevant control signal. The combiner **22** combines the output signal of the encoding unit **6** and the identification signal to form a composite signal. Subsequently, the composite signal is transmitted via the transmission medium. By selecting that version of the digital information signal having the smaller number of bits in the composite signal, the transmitting device will make optimum use of the storage capacity on a record carrier or will make optimum use of the bandwidth of a transmission medium.

In the preceding paragraph it has been described how a digital information signal is transmitted using the transmitter in accordance with the invention. The digital information signal is then regarded as one signal. However, the digital information signal may include a plurality of signal portions. A signal portion may be one music item, but may, alternatively, be a group of consecutive samples of the digital information signal. The transmitter in accordance with the invention, also enables each individual signal portion to be transmitted coded or not coded using the encoder **7** or a switching element **9**. The transmitter then includes an identification signaler **18** which, for the whole digital information signal and/or each individual signal portion, determines which manner (i.e., encoded or not encoded) requires the least number of bits for transmitting the digital information signal via the transmission medium. For some of the signal portions, encoding will lead to data reduction. For other signal portions, encoding will lead to a data increase. The control signal will then alternately be of the first type or the second type, respectively, in such a manner that, the signal portions for which the data reduction provided by the encoder **7** is unsatisfactory do not appear in encoded form in the output signal of the encoding unit **6**, and the other signal portions do appear in encoded form in the output signal. The identification signal now includes a first component which indicates that, possibly, one signal portion appears in encoded form in the composite signal. Moreover, there is a second component, which, for each of the portions, specifies whether the signal portion appears in an encoded form or not, in this encoded form in the composite signal.

FIG. **2** shows an embodiment of a receiver in accordance with the invention, for receiving a composite signal TRM. A version of the digital information signal is derived from the composite signal TRM. An exact or a non-exact copy of the digital information signal will be derived depending on the coding used in the transmitter. The composite signal TRM is received at the input **60** of demultiplexer **62**. The demultiplexer **62** derives an output signal and an identification signal from the composite signal TRM. The output signal contains a version of the digital information signal, and is applied to an output **64**. The version of the digital information signal may include one or more signal portions of the digital information signal. A signal portion can be a track of a disc or a group of consecutive samples of the digital information signal. The identification signal, which specifies how the version of the digital information signal has been encoded, is supplied to an output **66**. The identification signal specifies for each signal portion whether or not it has been encoded.

Identifier **70** has an input **68** coupled to the output **66** of the demultiplexer **62**. Identifier **70** derives a control signal from the identification signal, which control signal is to be transferred to a control output **72**. A control signal of a first type is derived from the identification signal when the corresponding portion of the output signal at the output **66** of the demultiplexer **62** has been encoded by the encoder. A control signal of a second type is derived from the identification signal, when the corresponding portion of the output signal at the output **66** of the demultiplexer **62** has not been encoded by the encoder.

The decoding unit **76** has an input **74** coupled to the output **64** of the demultiplexer **62**. A control input **78** is coupled to the control output **72** of the identifier **70**. The decoding unit **76** includes a decoder **77** to decode the signal received at the input **74** into a decoded signal, and includes switching element **79**. Depending on the control signal applied to the control input **78**, the switch **79** couples an output of the decoder **77** or the input **74** to the output **80**. As a result, the output signal of the decoding unit **76** includes a decoded version of the signal received at the input **74**, or the output signal is just the signal received at the input **74**. If the transmitter uses a lossless coding, the signal applied to the output **80** will be an exact copy of the digital information signal applied to the input of the transmitter. The decoder can be a lossy decoder or a lossless decoder. An example of a lossless decoder is described in the AES preprint 4563 “Improved Lossless Coding of 1-Bit Audio Signals” by Fons Bruekers et al., 103rd AES Convention (New York, US). The decoded signal is applied to the output **80** in response to a control signal of the first type. The signal is received at the input **74** is applied to the output **80** in substantially unmodified form, in response to a control signal of the second type. A signal may include a signal component of the digital information signal, or the entire digital information signal. The decoding unit **76** has its output **80** coupled to the output terminal **82**.

The receiver shown in FIG. **2** operates as follows. In the demultiplexer **62** a version of the digital information signal and an identification signal are derived from the composite signal TRM. The identifier derives a control signal from the identification signal. The identification signal has a first component which indicates whether one or several portions of the version of the digital information signal appear in the version encoded in a given manner. If the first component is not present, the version of the digital information signal is the version of the digital information signal which has not been encoded in the given manner. The first component can be recorded in a Table of Content, Track List or Block Header of, for example, a record carrier in the form of an optical disc. If the first component is present, the identification signal includes a second component. The second component specifies how the corresponding signal portion appears in encoded form in the version of the digital information signal. The control signal is generated depending on the first and the second component. The control signal determines whether or not the signal applied to the input **74** must be decoded before it is applied to the output **80**.

FIG. **3** shows a transmitter in the form of a recording apparatus for recording the digital information signal on a record carrier. The circuit block **300** in FIG. **3** is equivalent to the block diagram of FIG. **1**. The output **28** of the circuit block **300** corresponds to the output **28** of the combiner **22** in FIG. **1**. The recording apparatus further includes an error correction encoder **302**, a channel encoder **304**, and a writer **306** for writing the signal onto the record carrier **308**. Error correction encoders and channel encoders are generally known from the related art. The record carrier **308** can be of the magnetic type. In the present case, the writer **306** includes one or several magnetic heads **310** to record the information in a track on the record carrier **308**. In another embodiment, the record carrier **308** is an optical information carrier **308**'. In this case, the writer **306** includes an optical recording head **310** for recording the information in a track on the record carrier **308**'.

FIG. **4** shows a reproducing receiver for reproducing the digital information signal on the record carrier. The circuit block **400** in FIG. **4** is equivalent to the block diagram of FIG. **2**. The input **60** of the circuit block **400** corresponds to the input **60** of the demultiplexer **62** in FIG. **2**. The reproducing receiver further includes a reader **402**, a channel decoder **406** and an error detector **408** for detecting or, if possible, an error corrector **408** for correcting errors in the signal. Channel decoders and error detectors/correctors are generally known from the related art. The reader **402** reads the signal recorded on the record carrier **402***b* and supplies the signal thus read to a channel decoder **406**. The record carrier **402***b* can be of the magnetic type. In the present case, the reader **402** includes one or several magnetic read heads **402***a* for reading the information from a track on the record carrier **402***b*. In another embodiment, the record carrier **402***b* is an optical information carrier **402***b*'. In this case, the reader **402** includes an optical read head **402***a* for reading the information from a track on the record carrier **402***b*'.

A transmitter and a receiver, in accordance with the invention, often process the signals in a byte-oriented fashion. The first component of the identification signal can be recorded in, for example, the Table of Content, Track List or Block Headers. The second component of the identification signal can be recorded at the beginning of each signal portion in the composite signal, for example, at the beginning of each frame. A frame includes a part of the digital information signal and the parameters intended for the receiving device. As a result of the byte-oriented processing, it is desirable that each frame begins at a boundary of a byte or a plurality of bytes. When a signal portion appears in the composite signal in an encoded form, this portion in the composite signal may start with parameters which specify how the subsequent group of bits in the signal should be decoded. In the present case, the bits are processed separately and, consequently, the second component may include only one bit for this signal portion. The number of bits of an encoded signal need not correspond to an integral number of bytes. In order to ensure that the next portion of the composite signal begins at a byte boundary, it may be necessary to insert a number of bits at the end of the encoded signal in the composite signal. When a signal portion appears in the composite signal in a non-encoded form, i.e. in the original form, the second component may require one bit or one byte of space per signal portion, depending on the signal processing that is used. In the case that a byte-oriented signal processing is used, and a signal portion includes an integral number of bytes, the second component preferably occupies one byte of space. As a result, the boundaries of portions of the composite signal remain at the byte boundaries.

FIG. **5** shows a structure of the volume space on a record carrier in accordance with the invention. The volume space on the record carrier has been divided into: a File System Area, Master TOC Area, 2-Channel Stereo Area, Multi Channel Area, and Extra Data Area. The 2-Channel Stereo Area and the Multi Channel Area are referred to as Audio Areas. Each record carrier should have the Master TOC Area and at least one Audio Area. The record carrier may optionally have a File System Area. In this case, the File System Area includes a file system in accordance with the ISO 9660, File and Directory Naming Standard, and/or the Unit Data File (UDF) specification. ISO 9660 specifies the volume and file structure of record carriers in the form of a CD-ROM. The Extra Data Area may optionally be used for storing audio-related information. If the record carrier has an Extra Data Area, the record carrier should have a UDF and/or an ISO 9660 file. The data in the Extra Data Area can be addressed via the file system. The file system is stored in the File System Area. If the File System Area is not large enough to store the file system, the remainder of the file system can be stored in the Extra Data Area.

The Master TOC Area includes three identical copies of the Master TOC. The Master TOC describes the record carrier at the highest level. The three copies of the Master TOC are situated at the same location on each record carrier and have a fixed size of 10 sectors. A sector has a size of 2048 bytes. The first sector includes general information about the record carrier, such as the size and the location of the Audio Areas on the record carrier, album information, catalog number, type of record carrier, and the date of the record carrier.

FIG. **6** shows a structure of an Audio Area on the record carrier. The Audio Area includes a Track Area having Audio Tracks containing audio information, and an Area TOC with control information. All 2-channel stereo Audio Tracks are arranged in the 2-channel stereo Area. All Multi Channel Tracks are arranged in the Multi channel Area. Each Audio Area includes an Area TOC-**1**, a Track Area with Audio tracks, and an Area TOC-**2**. The content of the Area TOC-**1** and of the Area TOC-**2** is identical and includes a copy of the Area TOC. The location of the Area TOC-**1** and the Area TOC-**2** of each Audio Area is defined in the Master TOC.

The information stored in a Track Area is a Byte Stream. A Byte Stream is stored in an integral number of sectors. A sector used by a Byte Stream is called an Audio Sector. A Byte Stream is divided into Multiplexed Frames having a duration of 1⁄75 second. A Byte Stream includes an integral number of Multiplexed Frames and is the succession of all Multiplexed Frames in an Audio Area. FIG. **7** shows a layout of an Audio Sector. An Audio Sector includes a fixed number of bytes, for example, 2048 bytes. Each Audio Sector begins with an Audio Header and is followed by at least one Packet. If the last byte of a Packet in an Audio Sector does not lie within the last byte of an Audio Sector, Stuffing or Padding bytes are added up to the last byte of an Audio Sector. A Packet can contain only one of the following data types, namely Audio Data, Supplementary Data, or Padding Data. A Packet of Audio Data is called an Audio Packet. A Packet of Supplementary Data is called a Supplementary Packet. A Packet of Padding Data is called a Padding Packet. A packet can belong to only one Audio Sector. An Audio Sector should include at least one packet. An Audio Sector includes a maximum of seven Packets.

A Multiplexed Frame includes an integral number of Packets. A Multiplexed Frame should include at least one Audio Packet. In addition, a Multiplexed Frame may include Supplementary Data Packets and Padding Packets. An Audio Frame includes the concatenated Audio Packets in a Multiplexed Frame. A Supplementary Data Frame includes the concatenated Supplementary Data Packets in a Multiplexed Frame. A Padding Frame includes the concatenated Padding Packets in a Multiplexed Frame. Audio Frames, Supplementary Data Frames and Padding Frames are referred to as Elementary Frames.

Each Multiplexed Frame has a time code expressed in minutes, seconds, and the sequence number of the frame in the second. The first Audio Frame in the Track Area of an Audio Area has the time code **0**. The time code is incremented in each subsequent Multiplexed Frame in the entire Track Area.

FIG. **8** shows the relationship between Multiplexed Frames and Audio Sectors. The Audio Frames are shown at the top. The Audio Frames can be of different lengths when the Audio Frames have been obtained by lossless coding. These Audio Frames are divided into Audio Packets. In FIG. **8**, the Audio Frames N are divided into four Packets (N,**0**), (N,**1**), (N,**2**) and (N,**3**). The Audio Packets are subsequently arranged in the Audio Sectors. As stated hereinbefore, each Audio Sector begins with an Audio Header, followed by at least one Packet. In FIG. **8**, the Supplementary Data Packets are referenced S, the Padding packets are referenced p, and the Audio Headers are referenced h. Thus, in FIG. **8**, the Audio Sector M+3 includes an Audio Header, Audio Packet (N,**3**), Supplementary Data Packet N, Audio Packet (N+1,0), Supplementary Data Packet N+1, Padding Frame N+1 and Audio Frame (N+2,0).

The Area TOC includes control information for the Track Area of the Audio Area belonging to the Area TOC. Control information can, for example, include: the Byte__Rate of the Multiplexed data in the Audio Area expressed as the number of bytes per second, the sample rate used for the Audio Area, and the frame format. The frame format defines the frame structure of the multiplexed audio signal in the Track Area. Possible types of frame formats are, for example, Multi Channel flexible Format plain DSD, Fixed format 2-channel stereo plain DSD 3 frames in 14 sectors, Fixed format 2-channel stereo plain DSD 3 frames in 16 sectors, or Lossless encoded flexible format. In the case that the frame format indicates that the frame structure has the Lossless encoded flexible format, then at least one frame in the Track Area may have been Lossless encoded.

An Audio Sector begins with an Audio Header and is followed by at least one Packet. The Audio Header includes information about the Audio Sector, such as the number of Packets in the Audio Sector, the number of Audio Frames which begin in the Audio Sector, and a parameter which indicates whether the Audio Area to which the Audio Sector belongs has or does not have a frame format of the Lossless encoded flexible type. This parameter has been included in order to preclude some errors which can occur during reproduction of the Audio signals. The Audio Sector is the smallest unit that can be read from the information carrier. When the data on the record carrier is read using the file system, then the Audio Sectors can be read directly, and it is not necessary to first read the Area TOC belonging to the Audio Area in which the Audio sector lies. This makes it possible, to first, read an Audio Sector having a frame structure of the type Fixed format 2-channel stereo plain DSD 3 frames in 14 sectors. The audio signals are then of the DSD type. DSD signals are 1-bit signals and can be applied directly to the output of the receiving device. If after reading of the aforementioned Audio Sector, an Audio Sector is read which has a frame structure of the Lossless encoded flexible format type, the audio signals in this audio sector can be lossless encoded. If the lossless encoded signal is applied to the output, the applied signal may damage loudspeakers coupled to the receiving device. Therefore, during the read-out of each Audio Sector, the receiving device must be capable of detecting whether the read-out data has been or has not been lossless encoded so as to enable the data thus read to be processed correctly.

In addition to information about the Audio Sector, the Audio Header also includes information about each Packet in the Audio Sector and information about each frame that begins in the Audio Sector. Information about an Audio Packet can be, for example, an indication whether the Packet is the first Packet of a Frame, the type of data in the Packet, and the length of the Packet. The length can be represented, for example, as the number of bytes in the Packet. A Packet can contain only one data type, for example Audio Data, Supplementary Data, or Padding Data. For each frame that begins in the Audio Sector, the Audio Header contains frame information. Thus, each frame contains a time code. If the frame format is of the Lossless encoded flexible format type, the Audio Header of each frame which starts in the sector specifies the number of audio channels used, for example, 2, 5 or 6 channels, and the number of audio sectors (N__sectors) over which the starting frame has been divided. If, for example, the first Packet of a Frame starts somewhere in sector X and the last packet is situated in Audio Sector Y, N__sectors is equal to Y−X+1. Before a receiving device can decode the Lossless encoded data, it should first read all the packets belonging to a Frame. For this purpose, the information N-sectors is relevant.

An Audio Stream also includes the DSD audio signal in lossless encoded or non-lossless encoded form. An Audio Stream is the concatenation of all the Audio Frames in a Byte Stream. A Lossless encoded Audio Frame has a variable length. An Audio Frame, in an Audio Area for which the Area TOC specifies that the frame format is of the Lossless encoded flexible format type, starts with a bit that indicates whether the Audio Data appears in the Audio Frame in lossless encoded or non-lossless encoded form. Thus, it is possible that the Area TOC indicates, that the frame format is of the Lossless encoded flexible format type, and that all Audio Frames contain the Audio Data in non-lossless encoded form.

An apparatus in accordance with the invention may include both a transmitting device and a receiving device. The combination of the apparatuses shown in FIG. **4** and FIG. **5** yields an apparatus using a digital information signal can be recorded on the record carrier, and the recorded digital information signal can be read form the record carrier and can be reproduced at a later instant. Another possibility, is that two apparatuses, which both include a transmitting and receiving device, communicate with one another via one or several transmission media. Using its transmitting device, the first apparatus transmits a digital information signal to the second apparatus via a first transmission medium. The second apparatus receives this signal using the receiving device and transfers it to the output. In a similar manner the second apparatus can transmit a digital information signal to the second apparatus via a second transmission medium.

Depending on the physical implementation of the transmission medium use will be made of one or more transmission media.

What is claimed is:

1. A transmitter comprising:

input means for receiving a digital information signal;

means for encoding the digital information signal and generating an output signal including: portions of the output signal in the form of encoded portions of the digital information signal under the influence of a control signal of a first type, and portions of the output signal in the form of portions of the digital information signal under the influence of a control signal of a second type;

control means for generating the control signal of the first type and the control signal of the second type;

means for generating: a first identification signal of a first type which indicates that the output signal possibly includes a portion of the digital information signal which has been encoded in the encoding means; and a first identification signal of a second type which indicates that the output signal does not include any portions of the digital information signal which have been encoded by the encoding means;

means for generating, for a portion of the digital information signal: a second identification signal of a first type depending on the control signal of the first type and the first identification signal of the first type; and a second identification signal of a second type depending on the control signal of the second type and the first identification signal of the first type;

combining means for combining the output signal of the encoding means, the first identification signal and, if the first identification signal is of the first type, the second identification signal, so as to obtain a composite signal to be applied to a transmission medium.

2. The transmitter of claim **1**, further comprising means for determining whether encoding of a portion of the digital information signal leads to a data reduction by at least a predetermined factor, and for generating the control signal of the first type if encoding of the portion of the digital information signal leads to a data reduction larger than the predetermined factor.

3. The transmitter of claim **1**, further comprising:

at least one of error correction means for error encoding of the composite signal into an error-encoded signal and channel encoding means for channel encoding of the composite signal into a channel-encoded signal; and

recording means for recording at least one of the error-encoded signal and the channel-encoded signal on a record carrier.

4. The transmitter of claim **1**, further comprising:

means for determining whether encoding of a portion of the digital information signal leads to a data reduction by at least a predetermined factor, for generating the control signal of the first type if encoding of the portion of the digital information signal leads to a data reduction larger than the predetermined factor;

at least one of error correction means for error encoding of the composite signal into an error encoded signal and channel encoding means for channel encoding of the composite signal into a channel-encoded signal; and

recording means for recording at least one of the error-encoded signal and the channel-encoded signal on a record carrier.

5. A method comprising the steps of:

receiving a digital information signal;

encoding the digital information signal, depending on a composite control signal, to produce an output signal;

generating the composite control signal, including a first control signal of a first type and a second control signal of a second type;

generating portions of the output signal in the form of encoded portions of the digital information signal under the influence of said first control signal;

generating portions of the output signal in the form of portions of the digital information signal under the influence of said second control signal;

generating: a first identification signal of a first type which indicates that the output signal possibly includes a portion of the digital information signal which has been encoded; or a first identification signal of a second type which indicates that the output signal does not include any portions of the digital information signal which have been encoded;

generating a second identification signal of a first type depending on the first control signal and the a first identification signal of the first type;

generating a second identification signal of a second type depending on the second control signal and the first identification signal of the first type;

combining the output signal, the first identification signal and, if the first identification signal is of the first type, the second identification signal so as to obtain a composite signal;

applying the composite signal to a transmission medium.

6. The method claim **5**, further comprising the steps of:

producing at least one of an error correction encoded signal of the composite signal and a channel encoded signal of the composite signal; and

applying at least one of the error correction encoded signal and the channel encoded signal to the transmission medium.

7. The method of claim **5**, in which the transmission medium is a record carrier.

8. A record carrier obtained by the method of claim **7**, in which the record carrier is an optical or magnetic recording medium.

9. The method of claim **5**, further comprising the steps of:

producing at least one of an error correction encoded signal of the composite signal and a channel encoded signal of the composite signal; and

applying at least one of the error correction encoded signal and the channel encoded signal to the transmission medium; and

providing a transmission medium which is a record carrier.

10. A transmitter/receiver apparatus, for transmitting a digital information signal via a transmission medium, comprising:

a record carrier;

a digital information signal embodied on said record carrier, said digital information signal having portions which have been or have not been encoded using an encoding method; and

a first identification signal of a first type, wherein said first identification signal indicates that the digital information signal has been encoded using the encoding method.

11. The record carrier of claim **10**, further comprising a second identification signal for each portion of the digital information signal; and

in which: a second identification signal of a first type indicates for a portion of the digital information signal, that this portion has been encoded by means of the given encoding method; and a second identification signal of a second type indicates for a portion of the digital information signal, that this portion has not been encoded by means of the given encoding method.

12. The record carrier of claim **10** in which:

the record carrier further comprises a disc carrying digital information including at least one data area, each data area including a table of contents and a track area divided into frames each including a portion of a representation of the digital information signal;

the table of contents contains a first identification signal of a first or a second type, said first identification signal of said second type indicating that each frame in the track area contains a portion of the digital information signal which has not been encoded using the given encoding method, and said first identification signal of said first type indicating that a frame in the track area possibly contains a portion of the digital information signal which has been encoded using the given encoding method; and

if a data area contains said first identification signal of said first type, each frame includes a second identification signal which indicates whether the frame contains a portion of the digital information signal which has been or has not been encoded by means of the given encoding method.

13. The record carrier of claim **10**, in which:

the record carrier further comprises a second identification signal for each portion of the digital information signal;

a second identification signal of a first type indicates for a portion of the digital information signal, that this portion has been encoded by means of the given encoding method; and a second identification signal of a second type indicates for a portion of the digital information signal, that this portion has not been encoded by means of the given encoding method;

the record carrier further comprises a disc carrying digital information including at least one data area, each data area comprising a table of contents and a track area divided into frames each including a portion of a representation of the digital information signal;

the table of contents contains a first identification signal of a first or a second type, said first identification signal of said second type indicating that each frame in the track area contains a portion of the digital information signal which has not been encoded using the given encoding method, and said first identification signal of said first type indicating that a frame in the track area possibly contains a portion of the digital information signal which has been encoded using the given encoding method; and

if a data area contains said first identification signal of said first type, each frame includes a second identification signal which indicates whether the frame contains a portion of the digital information signal which has been or has not been encoded by means of the given encoding method.

14. A receiver comprising:

receiving means for receiving a composite signal from a transmission medium;

demultiplexing means for deriving at least one signal portion from the composite signal and for deriving a first identification signal of a first type and a second type from the composite signal;

decoding means for decoding at least one signal portion and for decoding a signal portion into a portion of the digital information signal and to supply the portion of a digital information signal depending on a control signal of a first type and to supply a signal portion as a portion of the digital information signal in a substantially unmodified form depending on a control signal of a second type; and

means for generating the control signal for application to the decoding means including a control signal of the first type depending on the first identification signal of the first type.

15. The receiver of claim **14**, in which:

the demultiplexing derive a first identification signal of a second type from the composite signal; and

the means for generating the control signal generate a control signal of the second type depending on the first identification signal of the second type.

16. The receiver of claim **14**, in which:

the demultiplexing means derive, depending on the identification signal of the first type, a second identification signal associated with each individual signal portion; and

the means for generating the control signal generate a control signal of the first type depending on the second identification signal of the first type and generate a control signal of the second type depending on the second identification signal of the second type.

17. A receiving device as claimed in claim **14**, in which the receiver further comprises:

a device for reading out a signal recorded on a record carrier; and

at least one of channel decoding means for the channel decoding of the read-out signal and error detection/correction means detecting and correcting errors in the read-out signal.

18. The receiver of claim **14**, in which:

the demultiplexing means derive a first identification signal of a second type from the composite signal;

the means for generating the control signal generate a control signal of the second type depending on the first identification signal of the second type;

the demultiplexing means derive, depending on the identification signal of the first type, a second identification signal associated with each individual signal portion;

the means for generating the control signal generate a control signal of the first type depending on the second identification signal of the first type, and generate a control signal of the second type depending on the second identification signal of the second type; and

the receiver further comprises:

- a device for reading out a signal recorded on a record carrier; and
- at least one of channel decoding means for the channel decoding of the read out signal and error detection/correction means for detecting and correcting errors in the read-out signal.

* * * * *

7

US008543819B2

(12) **United States Patent**
Kamperman

(10) **Patent No.: US 8,543,819 B2**
(45) **Date of Patent: Sep. 24, 2013**

(54) **SECURE AUTHENTICATED DISTANCE MEASUREMENT**

(75) Inventor: **Franciscus Lucas Antonius Johannes Kamperman**, Eindhoven (NL)

(73) Assignee: **Koninklijke Philips N.V.**, Eindhoven (NL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 34 days.

(21) Appl. No.: **12/508,917**

(22) Filed: **Jul. 24, 2009**

(65) **Prior Publication Data**

US 2009/0287927 A1 Nov. 19, 2009

Related U.S. Application Data

(63) Continuation of application No. 10/521,858, filed as application No. PCT/IB03/02932 on Jun. 27, 2003.

(30) **Foreign Application Priority Data**

Jul. 26, 2002 (EP) 02078076

(51) **Int. Cl.**
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
USPC **713/170**; 713/168; 713/156

(58) **Field of Classification Search**
USPC 713/150–153, 155–157, 160–161, 713/168, 170–171, 181; 726/2–10
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,438,824	A	3/1984	Mueller-Schloer	
4,688,036	A *	8/1987	Hirano et al.	340/5.62
5,126,746	A	6/1992	Gritton	
5,723,911	A *	3/1998	Glehr	340/10.5
5,778,071	A *	7/1998	Caputo et al.	713/159
5,937,065	A *	8/1999	Simon et al.	380/262
5,949,877	A *	9/1999	Traw et al.	713/171
5,983,347	A *	11/1999	Brinkmeyer et al.	340/5.62
6,085,320	A *	7/2000	Kaliski, Jr.	713/168
6,088,450	A *	7/2000	Davis et al.	713/182

(Continued)

FOREIGN PATENT DOCUMENTS

JP	4306760 A	10/1992
JP	6019948 A	1/1994

(Continued)

OTHER PUBLICATIONS

Boyd, Colin et al. "Protocols for Authentication and Key Establishment," Sep. 17, 2003, Springer-Verlag, p. 116-120, 195-196, 305.*

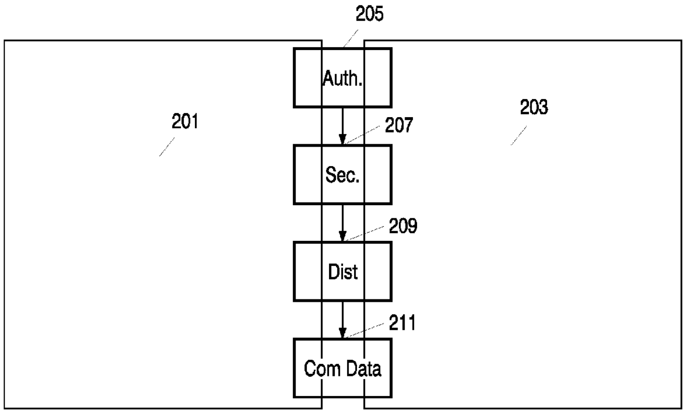
(Continued)

Primary Examiner — Darren B Schwartz

(57) **ABSTRACT**

The invention relates to a method for a first communication device to performing authenticated distance measurement between said first communication device and a second communication device, wherein the first and the second communication device share a common secret and said common secret is used for performing the distance measurement between said first and said second communication device. The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

16 Claims, 3 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,151,676	A	11/2000	Cuccia et al.	
6,208,239	B1 *	3/2001	Muller et al.	340/426.35
6,346,878	B1 *	2/2002	Pohlman et al.	340/435
6,484,948	B1	11/2002	Sonoda	
6,493,825	B1	12/2002	Blumenau et al.	
7,200,233	B1 *	4/2007	Keller et al.	380/268
2001/0008558	A1 *	7/2001	Hirafuji	380/220
2001/0043702	A1	11/2001	Elteto et al.	
2001/0044786	A1 *	11/2001	Ishibashi	705/77
2002/0007452	A1 *	1/2002	Traw et al.	713/152
2002/0026424	A1 *	2/2002	Akashi	705/57
2002/0026576	A1 *	2/2002	Das-Purkayastha et al. .	713/156
2002/0035690	A1 *	3/2002	Nakano	713/171
2002/0061748	A1 *	5/2002	Nakakita et al.	455/435
2002/0078227	A1 *	6/2002	Kronenberg	709/237
2003/0021418	A1 *	1/2003	Arakawa et al.	380/277
2003/0030542	A1 *	2/2003	von Hoffmann	340/5.61
2003/0065918	A1 *	4/2003	Willey	713/168
2003/0070092	A1 *	4/2003	Hawkes et al.	713/201
2003/0112978	A1 *	6/2003	Rodman et al.	380/277
2003/0184431	A1 *	10/2003	Lundkvist	340/5.2
2003/0220765	A1 *	11/2003	Overy et al.	702/158
2005/0114647	A1 *	5/2005	Epstein	713/153
2005/0265503	A1 *	12/2005	Rofheart et al.	375/354
2006/0294362	A1 *	12/2006	Epstein	713/153

FOREIGN PATENT DOCUMENTS

JP	9170364	A	6/1997
JP	2001257672	A	9/2001
WO	9739553	A1	10/1997
WO	0193434	A2	12/2001
WO	0233887	A2	4/2002
WO	0235036	A1	5/2002

OTHER PUBLICATIONS

Brands et al, “Distance-Bounding Protocols”, Eurocrypt ’93, 1993, pp. 344-359.

Kindberg et al, “Context Authentication Using Contrained Channels”, Undated, p. 108.

Hitachi, Ltd, “5C Digital Transmission Content Protection White Paper”, REV. 1.0, July 14, 1998, pp. 1-13.

* cited by examiner

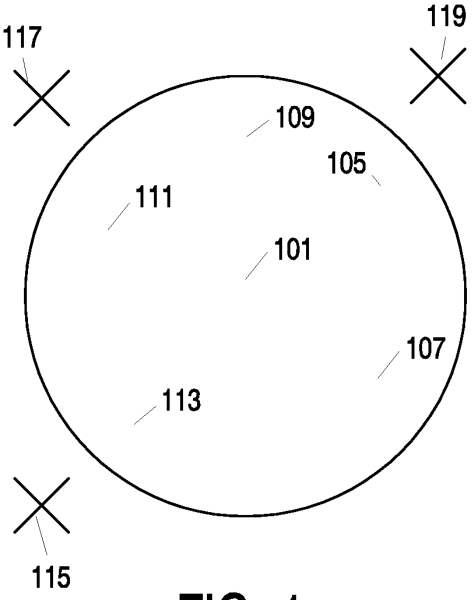

117
119
109
105
111
101
107
113
115

FIG. 1

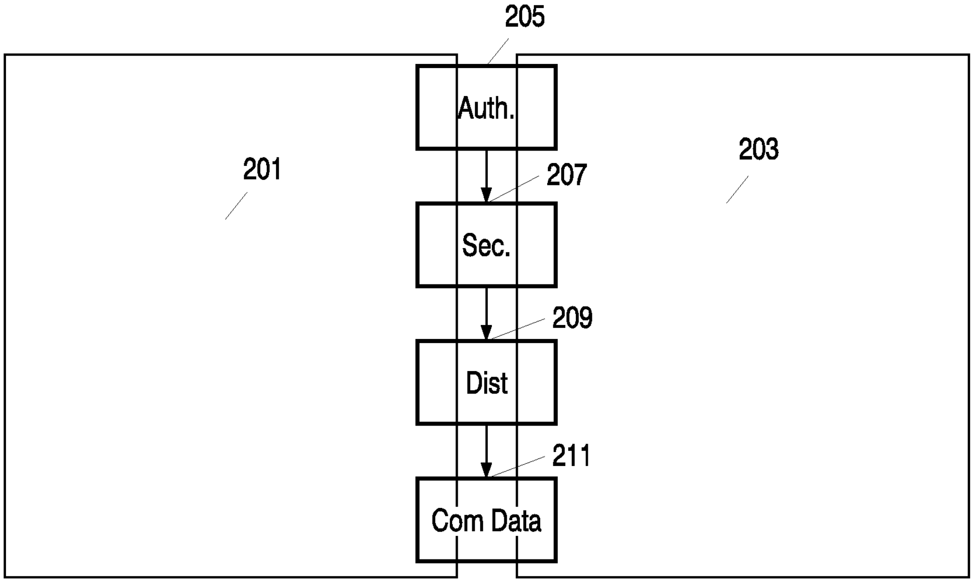

205
Auth.
201
207
203
Sec.
209
Dist
211
Com Data

FIG. 2

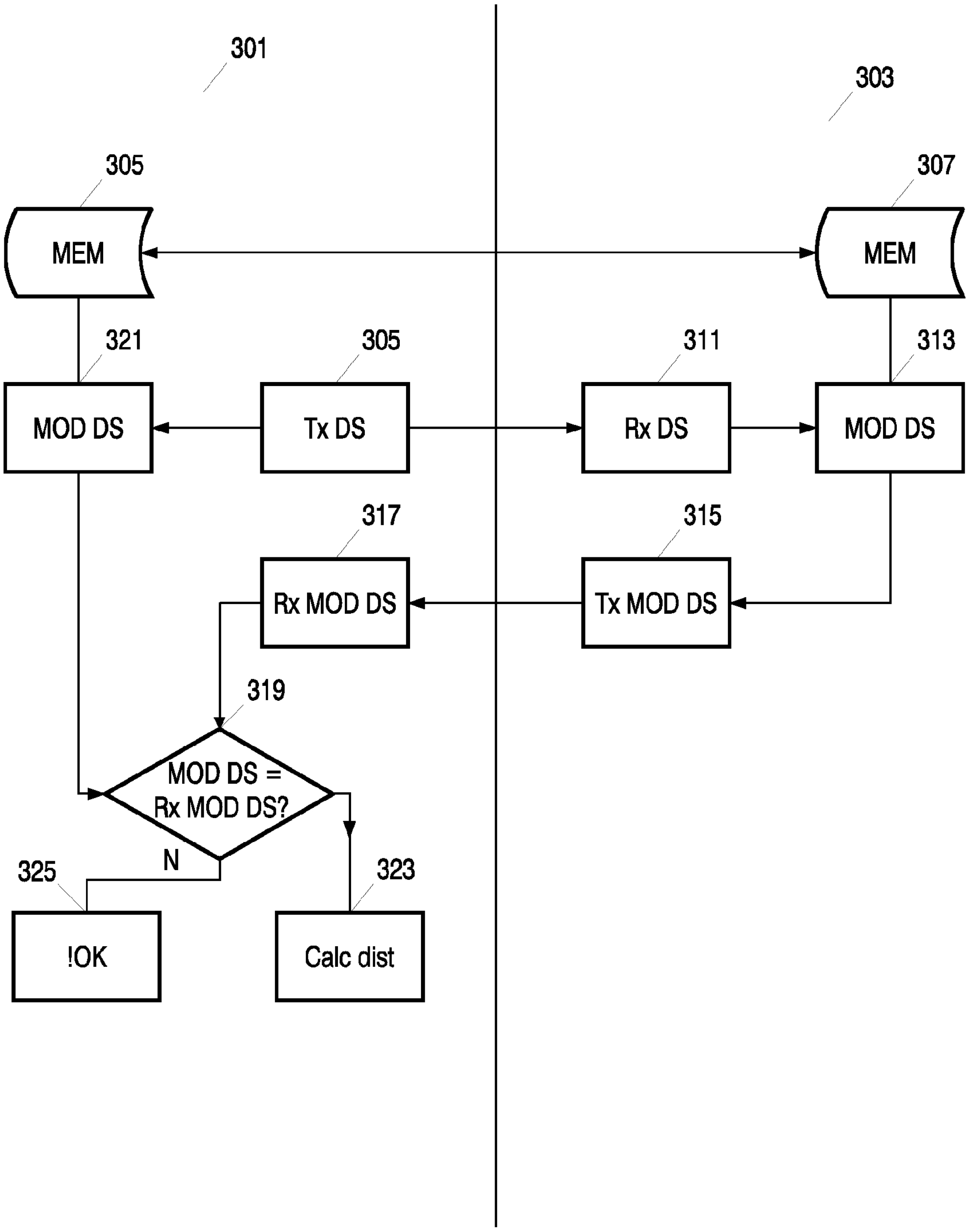

301
303
305
MEM
307
MEM
321
MOD DS
305
Tx DS
311
Rx DS
313
MOD DS
317
Rx MOD DS
315
Tx MOD DS
319
MOD DS =
Rx MOD DS?
N
325
!OK
323
Calc dist

FIG. 3

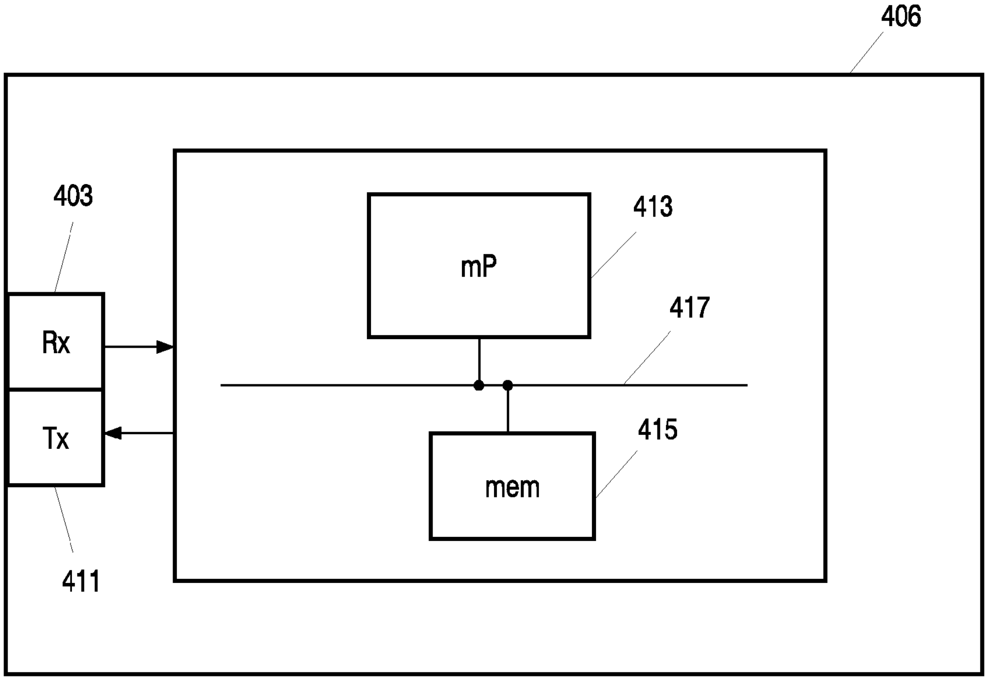


FIG. 4

SECURE AUTHENTICATED DISTANCE MEASUREMENT

The invention relates to a method for a first communication device to performing authenticated distance measurement between a first communication device and a second communication device. The invention also relates to a method of determining whether data stored on a first communication device is to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

Digital media have become popular carriers for various types of data information. Computer software and audio information, for instance, are widely available on optical compact disks (CDs) and recently also DVD has gained in distribution share. The CD and the DVD utilize a common standard for the digital recording of data, software, images, and audio. Additional media, such as recordable discs, solid-state memory, and the like, are making considerable gains in the software and data distribution market.

The substantially superior quality of the digital format as compared to the analog format renders the former substantially more prone to unauthorized copying and pirating, further a digital format is both easier and faster to copy. Copying of a digital data stream, whether compressed, uncompressed, encrypted or non-encrypted, typically does not lead to any appreciable loss of quality in the data. Digital copying thus is essentially unlimited in terms of multi-generation copying. Analog data with its signal to noise ratio loss with every sequential copy, on the other hand, is naturally limited in terms of multi-generation and mass copying.

The advent of the recent popularity in the digital format has also brought about a slew of copy protection and DRM systems and methods. These systems and methods use technologies such as encryption, watermarking and right descriptions (e.g. rules for accessing and copying data).

One way of protecting content in the form of digital data is to ensure that content will only be transferred between devices if

- the receiving device has been authenticated as being a compliant device,
- if the user of the content has the right to transfer (move, copy) that content to another device.

If transfer of content is allowed, this will typically be performed in an encrypted way to make sure that the content cannot be captured illegally in a useful format.

Technology to perform device authentication and encrypted content transfer is available and is called a secure authenticated channel (SAC). Although it might be allowed to make copies of content over a SAC, the content industry is very bullish on content distribution over the Internet. This results in disagreement of the content industry on transferring content over interfaces that match well with the Internet, e.g. Ethernet.

Further, it should be possible for a user visiting his neighbour to watch a movie, which he owns, on the neighbour's big television screen. Typically, the content owner will disallow this, but it might become acceptable if it can be proved that a license holder of that movie (or a device that the license holder owns) is near that television screen.

It is therefore of interest to be able to include an authenticated distance measurement when deciding whether content should be accessed or copied by other devices.

In the article by Stefan Brands and David Chaum, "Distance-Bounding protocols", Eurocrypt '93 (1993), Pages 344-359, integration of distance-bounding protocols with public-key identification schemes is described. Here distance measurement is described based on time measurement using challenge and response bits and with the use of a commitment protocol. This does not allow authenticated device compliancy testing and is not efficient when two devices must also authenticate each other.

It is an object of the invention to obtain a solution to the problem of performing a secure transfer of content within a limited distance.

This is obtained by a method for a first communication device to performing authenticated distance measurement between said first communication device and a second communication device, wherein the first and the second communication device share a common secret and said common secret is used for performing the distance measurement between said first and said second communication device.

Because the common secret is being used for performing the distance measurement, it can be ensured that when measuring the distance from the first communication device to the second communication device, it is the distance between the right devices that is being measured.

The method combines a distance measurement protocol with an authentication protocol. This enables authenticated device compliancy testing and is efficient, because a secure channel is anyhow needed to enable secure communication between devices and a device can first be tested on compliancy before a distance measurement is executed.

In a specific embodiment, the authenticated distance measurement is performed according to the following steps,

- transmitting a first signal from the first communication device to the second communication device at a first time **t1**, said second communication device being adapted for receiving said first signal, generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal to the first device,
- receiving the second signal at a second time **t2**,
- checking if the second signal has been modified according to the common secret,
- determining the distance between the first and the second communication device according to a time difference between **t1** and **t2**.

When measuring a distance by measuring the time difference between transmitting and receiving a signal and using a secret, shared between the first and the second communication device, for determining whether the returned signal really originated from the second communication device, the distance is measured in a secure authenticated way ensuring that the distance will not be measured to a third communication device (not knowing the secret). Using the shared secret for modifying the signal is a simple way to perform a secure authenticated distance measurement.

In a specific embodiment the first signal is a spread spectrum signal. Thereby a high resolution is obtained and it is possible to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In another embodiment the step of checking if the second signal has been modified according to the common secret is performed by the steps of,

- generating a third signal by modifying the first signal according to the common secret,
- comparing the third signal with the received second signal.

This method is an easy and simple way of performing the check, but it requires that both the first communication device and the second communication device know how the first signal is being modified using the common secret.

In a specific embodiment the first signal and the common secret are bit words and the second signal comprises information being generated by performing an XOR between the bit words. Thereby, it is a very simple operation that has to be performed, resulting in demand for few resources by both the first and the second communication device when performing the operation.

In an embodiment the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of,

performing an authentication check from the first communication device on the second communication device by checking whether said second communication device is compliant with a set of predefined compliance rules,

if the second communication device is compliant, sharing said common secret by transmitting said secret to the second communication device.

This is a secure way of performing the sharing of the secret, ensuring that only devices being compliant with compliance rules can receive the secret. Further, the shared secret can afterwards be used for generating a SAC channel between the two devices. The secret could be shared using e.g. key transport mechanisms as described in ISO 11770-3. Alternatively, a key agreement protocol could be used, which e.g. is also described in ISO 11770-3.

In another embodiment the authentication check further comprises checking if the identification of the second device is compliant with an expected identification. Thereby, it is ensured that the second device really is the device that it should be. The identity could be obtained by checking a certificate stored in the second device.

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between the first and the second communication device and checking whether said measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. By using the authenticated distance measurement in connection with sharing data between devices, unauthorised distribution of content can be reduced.

In a specific embodiment the data stored on the first device is sent to the second device if it is determined that the data stored on the first device are to be accessed by the second device.

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between a third communication device and the second communication device and checking whether said measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. In this embodiment, the distance is not measured between the first communication device, on which the data are stored, and the second communication device. Instead, the distance is measured between a third communication device and the second communication device, where the third communication device could be personal to the owner of the content.

The invention also relates to a communication device for performing authenticated distance measurement to a second communication device, where the communication device shares a common secret with the second communication device and where the communication device comprises means for measuring the distance to the second device using said common secret.

In an embodiment the device comprises,

means for transmitting a first signal to a second communication device at a first time **t1**, said second communication device being adapted for receiving said first signal, generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal,

means for receiving the second signal at a second time t**2**,

means for checking if the second signal has been modified according to the common secret,

means for determining the distance between the first and the second communication device according to a time difference between t**1** and t**2**.

The invention also relates to an apparatus for playing back multimedia content comprising a communication device according to the above.

In the following preferred embodiments of the invention will be described referring to the figures, wherein

FIG. **1** illustrates authenticated distance measurement being used for content protection,

FIG. **2** is a flow diagram illustrating the method of performing authenticated distance measurement,

FIG. **3** illustrates in further detail the step of performing the authenticated distance measurement shown in FIG. **2**,

FIG. **4** illustrates a communication device for performing authenticated distance measurement.

FIG. **1** illustrates an embodiment where authenticated distance measurement is being used for content protection. In the centre of the circle **101** a computer **103** is placed. The computer comprises content, such as multimedia content being video or audio, stored on e.g. a hard disk, DVD or a CD. The owner of the computer owns the content and therefore the computer is authorised to access and present the multimedia content for the user. When the user wants to make a legal copy of the content to another device via e.g. a SAC, the distance between the other device and the computer **103** is measured and only devices within a predefined distance illustrated by the devices **105**, **107**, **109**, **111**, **113** inside the circle **101** are allowed to receive the content. Whereas the devices **115**, **117**, **119** having a distance to the computer **101** being larger than the predefined distance are not allowed to receive the content.

In the example a device is a computer, but it could e.g. also be a DVD drive, a CD drive or a Video, as long as the device comprises a communication device for performing the distance measurement.

In a specific example the distance might not have to be measured between the computer, on which the data are stored, and the other device, it could also be a third device e.g. a device being personal to the owner of the content which is within the predefined distance.

In FIG. **2** a flow diagram illustrates the general idea of performing authenticated distance measurement between two devices, **201** and **203** each comprising communication devices for performing the authenticated distance measurement. In the example the first device **201** comprises content which the second device **203** has requested. The authenticated distance measurement then is as follows. In **205** the first device **201** authenticates the second device **203**; this could comprise the steps of checking whether the second device **203** is a compliant device and might also comprise the step of checking whether the second device **203** really is the device identified to the first device **201**. Then in **207**, the first device **201** exchanges a secret with the second device **203**, which e.g. could be performed by transmitting a random generated bit word to **203**. The secret should be shared securely, e.g. according to some key management protocol as described in e.g. ISO 11770.

Then in **209**, a signal for distance measurement is transmitted to the second device **203**; the second device modifies the received signal according to the secret and retransmits the modified signal back to the first device. The first device **201** measures the round trip time between the signal leaving and the signal returning and checks if the returned signal was modified according to the exchanged secret. The modification of the returned signal according to some secret will most likely be dependent on the transmission system and the signal used for distance measurement, i.e. it will be specific for each communication system (such as 1394, Ethernet, Bluetooth, ieee 802.11, etc.).

The signal used for the distance measurement may be a normal data bit signal, but also special signals other than for data communication may be used. In an embodiment spread spectrum signals are used to be able to get high resolution and to be able to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In a specific example a direct sequence spread spectrum signal is used for distance measurement; this signal could be modified by XORing the chips (e.g. spreading code consisting of 127 chips) of the direct sequence code by the bits of the secret (e.g. secret consists also of 127 bits). Also, other mathematical operations as XOR could be used.

The authentication **205** and exchange of secret **207** could be performed using the protocols described in some known ISO standards ISO 9798 and ISO 11770. For example the first device **201** could authenticate the second device **203** according to the following communication scenario:

First device->Second device: R_B||Text 1

where R_B is a random number

Second device->First device: CertA||TokenAB

Where CertA is a certificate of A

$\text{Token}AB=R_A||R_B||B||\text{Text3}||sS_A(R_A||R_B||B||\text{Text2})$

R_A is a random number
Identifier B is an option
sS_A is a signature set by A using private key S_A

If TokenAB is replaced with the token as specified in ISO 11770-3 we at the same time can do secret key exchange. We can use this by substituting Text2 by:

$\text{Text2}:=eP_B(A||K||\text{Text2})||\text{Text3}$

Where eP_B is encrypted with Public key B
A is identifier of A
K is a secret to be exchanged

In this case the second device **203** determines the key (i.e. has key control), this is also called a key transport protocol, but also a key agreement protocol could be used. This may be undesirable in which case it can be reversed, such that the first device determines the key. A secret key has now been exchanged according to **207** in FIG. **2**. Again, the secret key could be exchanged by e.g. a key transport protocol or a key agreement protocol.

After the distance has been measured in a secure authenticated way as described above content, data can be send between the first and the second device in **211**.

FIG. **3** illustrates in further detail the step of performing the authenticated distance measurement. As described above the first device **301** and the second device **303** have exchanged a secret; the secret is stored in the memory **305** of the first device and the memory **307** of the second device. In order to perform the distance measurement, a signal is transmitted to the second device via a transmitter **309**. The second device receives the signal via a receiver **311** and **313** modifies the signal by using the locally stored secret. The signal is modified according to rules known by the first device **301** and transmitted back to the first device **301** via a transmitter **315**. The first device **301** receives the modified signal via a receiver **317** and in **319** the received modified signal is compared to a signal, which has been modified locally. The local modification is performed in **321** by using the signal transmitted to the second device in **309** and then modifying the signal using the locally stored secret similar to the modification rules used by the second device. If the received modified signal and the locally modified signal are identical, then the received signal is authenticated and can be used for determining the distance between the first and the second device. If the two signals are not identical, then the received signal cannot be authenticated and can therefore not be used for measuring the distance as illustrated by **325**. In **323** the distance is calculated between the first and the second device; this could e.g. be performed by measuring the time, when the signal is transmitted by the transmitter **309** from the first device to the second device and measuring when the receiver **317** receives the signal from the second device. The time difference between transmittal time and receive time can then be used for determining the physical distance between the first device and the second device.

In FIG. **4** a communication device for performing authenticated distance measurement is illustrated. The device **401** comprises a receiver **403** and a transmitter **411**. The device further comprises means for performing the steps described above, which could be by executing software using a microprocessor **413** connected to memory **417** via a communication bus. The communication device could then be placed inside devices such as a DVD, a computer, a CD, a CD recorder, a television and other devices for accessing protected content.

The invention claimed is:

1. A method of determining whether protected content stored on a first communication device are accessed by a second communication device, the method comprising the step of:

performing a round trip time measurement between the first communication device and the second communication device, said round trip time measurement comprising:

transmitting a first signal to the second device at a first time;

receiving a second signal from the second device at a second time,

generating a third signal using a common secret;

determining whether said second signal and said third signal are identical to verify that the second signal was generated using the common secret;

generating the round trip time as a difference between said first time and said second time;

checking whether the round trip time is within a predefined interval, and allowing access of the protected content provided that the round trip time is within the predefined interval, said second signal and said third signal are identical and the second device is authenticated,

wherein:

the first device authenticates the second device by:

receiving a certificate of said second device;

verifying that the certificate of said second device identifies said second device as complying with a set of predefined compliance rules, and the first device securely shares the common secret with the second device according to a key management protocol after having authenticated the second device.

2. The method according to claim **1**, wherein the round trip time measurement comprises the steps of:

generating the second signal according to the common secret, and transmitting the second signal to the first device.

3. The method according to claim **2**, wherein the first signal and the common secret are bit words and where the second signal comprises modifying the first signal by performing an XOR of the first signal with the common secret.

4. The method according to claim **1**, wherein the authentication check of the second device further comprises the step of checking if the identification of the second device is compliant with an expected identification.

5. The method according to claim **1**, in which the key management protocol comprises one of a key transport protocol and a key agreement protocol.

6. The method according to claim **1**, wherein the common secret is securely shared with the second device by encrypting the common secret using a public key of a private/public key-pair.

7. The method according to claim **1**, wherein the protected content stored on the first device (**201**) is sent to the second device (**203**) if it is determined that the protected content stored on the first device (**201**) is permitted to be shared with the second device (**203**).

8. The method according to claim **1**, wherein securely sharing the common secret with the second device by the first device comprises transmitting a random generated bit word to the second device.

9. The method according to claim **1**, wherein the common secret is used for generating a secure channel between the first and the second communication device.

10. A first communication device configured for determining whether protected content stored on the first communication device is available for access by a second communication device, the first communication device comprising:

means for performing an authentication of the second communication device, the authentication of the second device comprises:

receiving a certificate of the second device;

verifying that that the certificate of said second device identifies the second device as complying with a set of predefined compliance rules;

means for securely sharing a common secret with the second communication device after the second communication device is authenticated;

means for performing a round trip time measurement between the first communication device and the second communication device comprising:

transmitting a first signal to said second device at time t**1**;

receiving at time t**2** a second signal from said second device, said second signal being generated using said common secret;

determining said round trip time measurement as a difference between time t**1** and time t**2**;

means for checking whether the measured round trip time is within a predefined interval,

means for generating a third signal using said common secret;

means for checking whether said second signal and said third signal are identical; and

means for allowing access to said protected content when said round trip time measurement is within the predefined interval and the second and third signals are identical.

11. The first communication device according to claim **10**, further comprising

means arranged to securely share the common secret with the second device by encrypting the common secret using a public key of a private/public key-pair.

12. The first communication device according to claim **10**, further comprising:

means for transmitting the first signal at a first time t**1**,

means for receiving the second signal at a second time t**2**,

means for determining a time difference between the first time t**1** and the second time t**2**.

13. A system for secure transfer of protected content comprising a first communication device in communication with a second communication device, the first communication device comprising:

a memory storing a common secret,

processing means:

performing an authentication of the second communication device comprising:

receiving a certificate of said second device;

checking whether the certificate of said second communication device is compliant with an expected identification of the second communication device;

securely sharing the common secret with the second communication device after the second communication device is authenticated;

generating a third signal using the common secret;

transmitting a first signal to the second communication device;

receiving a second signal from said second communication device;

checking whether said second and third signals are identical;

performing a round trip time measurement between the first communication device and the second communication device using times associated with the first and second signals,

checking whether the measured round trip time is within a predefined interval; and

transmitting the protected content to the second device depending on when the round trip time measurement is within the predefined interval and the second and third signals are identical.

14. A first device configured for determining whether protected content stored on a first communication device is available for access by a second communication device, the second device being adapted for receiving a first signal from the first device, generating a second signal according to a common secret, and transmitting the second signal to the first device, the first device comprising:

a transmitter;

a receiver;

a memory storing the common secret;

a bus connected to the memory;

a processor connected to the bus and controlling the transmitter and receiver, the processor executing the steps of:

measuring a round trip time between the first device and the second device, said measured round trip time being determined based on a time difference between signals transmitted between the first and second devices,

generating a third signal depending on the common secret;

determining whether the second signal received from the second device during the round trip measurement is identical to the third signal to verify that the second signal was generated using the common secret;

checking whether said measured round trip time is within a predefined interval,

authenticating the second device, the authentication of the second device including:

receiving a certificate of the second device; and

verifying that the certificate of the second device identifies the second device as complying with a set of predefined compliance rules; and

securely transmitting the common secret to the second device after the second device has been authenticated.

15. The first communication device of claim **14** wherein the processor securely shares the common secret with the second communication device by encrypting the common secret using a public key of a private/public key-pair.

16. The first communication device of claim **14** wherein the processor performs the round trip time measurement by:

transmitting a first signal from the first device to the second device at time t**1**, receiving the second signal from the second device at time t**2**,

and

determining a time difference between the first time t**1** and the second time t**2**.

* * * * *

8

US009436809B2

(12) **United States Patent**
Kamperman

(10) **Patent No.: US 9,436,809 B2**
(45) **Date of Patent: *Sep. 6, 2016**

(54) **SECURE AUTHENTICATED DISTANCE MEASUREMENT**

(71) Applicant: **KONINKLIJKE PHILIPS N.V.**, Eindhoven (NL)

(72) Inventor: **Franciscus Lucas Antonius Johannes Kamperman**, Geldrop (NL)

(73) Assignee: **KONINKLIJKE PHILIPS N.V.**, Eindhoven (NL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/538,493**

(22) Filed: **Nov. 11, 2014**

(65) **Prior Publication Data**

US 2015/0074822 A1 Mar. 12, 2015

Related U.S. Application Data

(63) Continuation of application No. 10/521,858, filed as application No. PCT/IB03/02932 on Jun. 27, 2003, now Pat. No. 8,886,939.

(30) **Foreign Application Priority Data**

Jul. 26, 2002 (EP) 02078076

(51) **Int. Cl.**

G06F 21/10	(2013.01)
H04L 29/06	(2006.01)

(Continued)

(52) **U.S. Cl.**

CPC ***G06F 21/10*** (2013.01); ***H04L 63/107*** (2013.01); *G06F 2221/07* (2013.01); *G06F 2221/2111* (2013.01); *H04L 2463/101* (2013.01); *H04W 12/06* (2013.01); *H04W 24/00* (2013.01)

(58) **Field of Classification Search**

CPC G06F 21/10; H04L 63/107
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,438,824	A	3/1984	Mueller-Schloer
4,688,036	A	8/1987	Hirano et al.

(Continued)

FOREIGN PATENT DOCUMENTS

JP	9170364	A	0/6199
JP	H04306760	A	10/1992

(Continued)

OTHER PUBLICATIONS

Stefan Brands and Devid Chaum, "Distance-Bounding Protocols", Eurocrypt '93 (1993), pp. 344-359.

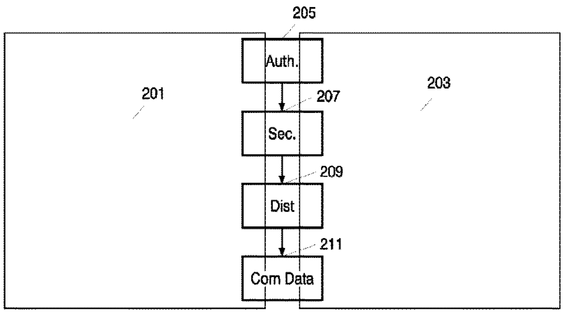
(Continued)

Primary Examiner — Darren B Schwartz

(57) **ABSTRACT**

The invention relates to a method for a first communication device to perform authenticated distance measurement between the first communication device and a second communication device, wherein the first and the second communication device share a common secret and the common secret is used for performing the distance measurement between the first and the second communication device. The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

60 Claims, 3 Drawing Sheets



(51) **Int. Cl.**

H04W 12/06	(2009.01)
H04W 24/00	(2009.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,126,746	A	6/1992	Gritton	
5,596,641	A	1/1997	Ohashi et al.	
5,602,917	A	2/1997	Mueller	
5,659,617	A *	8/1997	Fischer	H04L 9/3271 380/258
5,723,911	A	3/1998	Glehr	
5,778,071	A	7/1998	Caputo et al.	
5,937,065	A	8/1999	Simon et al.	
5,949,877	A	9/1999	Traw et al.	
5,983,347	A	11/1999	Brinkmeyer et al.	
6,085,320	A	7/2000	Kaliski, Jr.	
6,088,450	A	7/2000	Davis et al.	
6,151,676	A	11/2000	Cuccia et al.	
6,208,239	B1	3/2001	Muller et al.	
6,346,878	B1	2/2002	Pohlman et al.	
6,351,235	B1	2/2002	Stilp	
6,442,690	B1 *	8/2002	Howard, Jr.	G06F 21/602 713/156
6,484,948	B1	11/2002	Sonoda	
6,493,825	B1	12/2002	Blumenau et al.	
6,526,509	B1 *	2/2003	Horn	H04L 9/3263 380/277
6,550,011	B1 *	4/2003	Sims, III	G06F 21/10 365/52
7,200,233	B1	4/2007	Keller et al.	
8,107,627	B2	1/2012	Epstein	
8,352,582	B2	1/2013	Epstein	
8,997,243	B2	3/2015	Epstein	
2001/0008558	A1	7/2001	Hirafuji	
2001/0043702	A1	11/2001	Elteto et al.	
2001/0044786	A1	11/2001	Ishibashi	
2001/0050990	A1 *	12/2001	Sudia	G06Q 20/02 380/286
2002/0007452	A1	1/2002	Traw et al.	
2002/0026424	A1	2/2002	Akashi	
2002/0026576	A1	2/2002	Das-Purkayastha et al.	
2002/0035690	A1	3/2002	Nakano	
2002/0061748	A1	5/2002	Nakakita et al.	
2002/0078227	A1	6/2002	Kronenberg	
2002/0166047	A1 *	11/2002	Kawamoto	H04L 9/3263 713/169
2003/0021418	A1	1/2003	Arakawa et al.	
2003/0030542	A1	2/2003	von Hoffmann	
2003/0051151	A1 *	3/2003	Asano	G11B 20/00086 713/193
2003/0065918	A1	4/2003	Willey	
2003/0070092	A1	4/2003	Hawkes et al.	
2003/0112978	A1	6/2003	Rodman et al.	
2003/0184431	A1	10/2003	Lundkvist	
2003/0220765	A1	11/2003	Overy et al.	
2004/0015693	A1	1/2004	Kitazumi	
2004/0080426	A1 *	4/2004	Fraenkel	H04W 8/245 340/9.14
2005/0114647	A1	5/2005	Epstein	
2005/0265503	A1	12/2005	Rofheart et al.	
2006/0294362	A1	12/2006	Epstein	

FOREIGN PATENT DOCUMENTS

JP	H0619948	A	1/1994
JP	H08234658	A	9/1996
JP	H09170364	A	6/1997
JP	11101035	A	4/1999
JP	11208419	A	8/1999
JP	2000357156	A	12/2000
JP	2001249899	A	9/2001
JP	2001257672	A	9/2001
JP	2002124960	A	4/2002
JP	2002189966	A	7/2002
WO	9739553	A1	10/1997
WO	9949378		9/1999
WO	0152234	A1	7/2001
WO	0193434	A2	12/2001
WO	0233887	A2	4/2002
WO	0235036	A1	5/2002

OTHER PUBLICATIONS

Tim Kindber & Kan Zhang, "Context Authentication Using Constrained Channels", pp. 1-8.

Hitachi, Ltd, "5C Digital Transmission Content Protection White Papter", Rev. 1.0, July 14, 1998, pp. 1013.

Boyd et al, "Protocols for Authentication and Key Establishment", Spring-Verlag, September 17, 2003, pp. 116-120, 195-195, 305.

Modern Cryptography Theory (1986) Chapter 9, ISBN: 4-88552-064-9 (Japanese).

Hayashi et al, Encyption and Authentication Program Module, Technical Paper (Japanese) NTT R&D vol. 44 No. 10 Oct. 1, 1995.

Ikeno et al. "Modern Cryptography Theory" Japan, Institute of Electronics, Information and Communication Engineersm Nov. 15, 1997, p. 175-177.

* cited by examiner

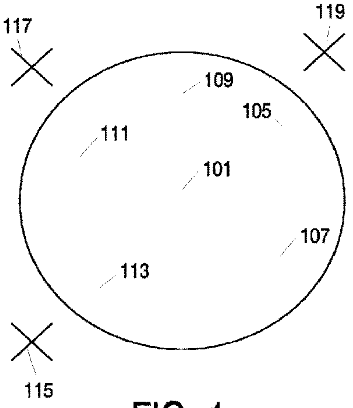

117
119
109
105
111
101
107
113
115

FIG. 1

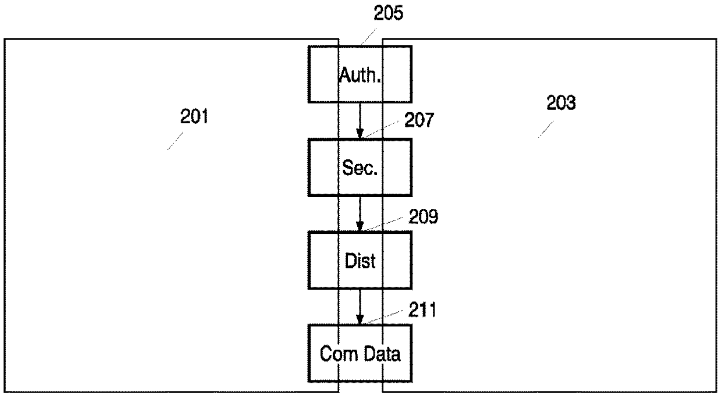

205
Auth.
201
207
203
Sec.
209
Dist
211
Com Data

FIG. 2

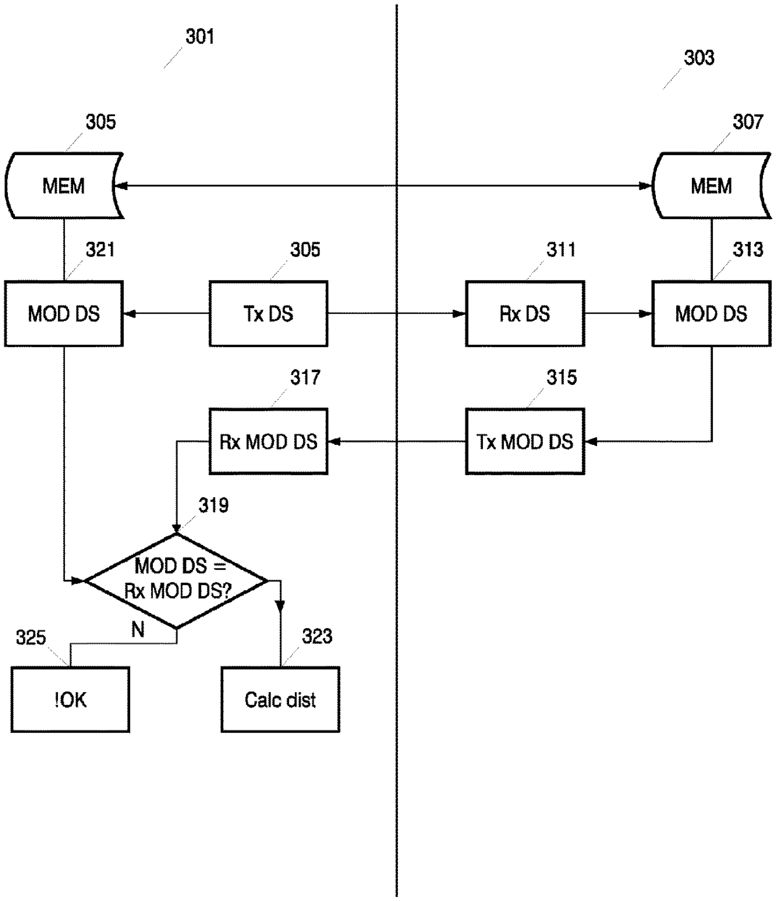

301
303
305
MEM
307
MEM
321
MOD DS
305
Tx DS
311
Rx DS
313
MOD DS
317
Rx MOD DS
315
Tx MOD DS
319
MOD DS = Rx MOD DS?
N
325
!OK
323
Calc dist

FIG. 3

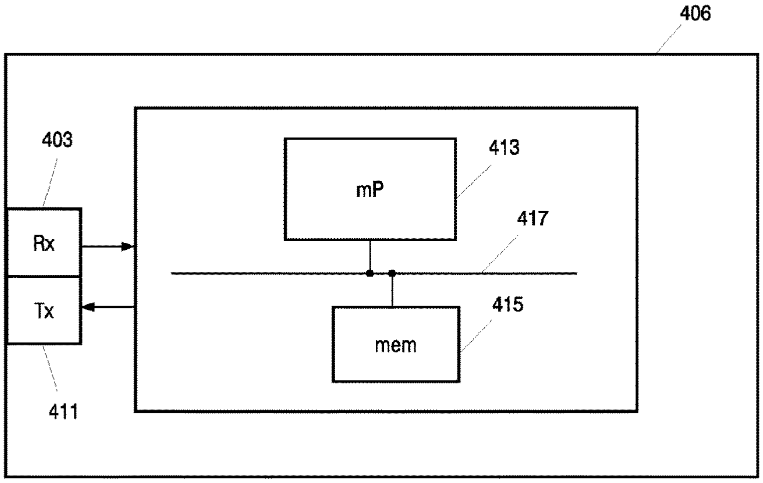


FIG. 4

SECURE AUTHENTICATED DISTANCE MEASUREMENT

This application claims, pursuant to 35 USC 120, priority to and the benefit of the earlier filing date of, that patent application entitled "Secure Authenticated Distance Measurement", filed on Jan. 21, 2005 and afforded Ser. No. 10/521,858 (now U.S. Pat. No. 8,886,939), which claimed priority to and the benefit of the earlier filing date, as a National Stage Filing of that international patent application filed on Jun. 27, 2003 and afforded serial number PCT/IB03/02932 (WO2004014037), which claimed priority to and the benefit of the earlier filing date of that patent application filed on Jul. 26, 2002 and afforded serial number EP02078076.3, the contents of all of which are incorporated by reference, herein.

This application is further related to that patent application entitled "Secure authenticated Distance Measurement", filed on Jul. 24, 2009 and afforded Ser. No. 12/508,917 (now U.S. Pat. No. 8,543,819), issued Sep. 24, 2013), which claimed priority to and the benefit of the earlier filing date of that patent application entitled "Secure Authenticated Distance Measurement", filed on Jan. 21, 2005 and afforded Ser. No. 10/521,858 (now U.S. Pat. No. 8,886,939), the contents of which are incorporated by reference herein.

The invention relates to a method for a first communication device to perform authenticated distance measurement between a first communication device and a second communication device. The invention also relates to a method of determining whether data stored on a first communication device is to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

Digital media have become popular carriers for various types of data information. Computer software and audio information, for instance, are widely available on optical compact disks (CDs) and recently also on digital video/versatile discs (DVDs) which have been gaining in distribution share. The CD and the DVD utilize a common standard for the digital recording of data, software, images, audio and multimedia. Additional media, such as recordable discs, solid-state memory, and the like, are making considerable gains in the software and data distribution market.

The substantially superior quality of the digital format as compared to the analog format renders the former substantially more prone to unauthorized copying and pirating, further a digital format is both easier and faster to copy. Copying of a digital data stream, whether compressed, uncompressed, encrypted or non-encrypted, typically does not lead to any appreciable loss of quality in the data. Digital copying thus is essentially unlimited in terms of multi-generation copying. Analog data with its signal to noise ratio loss with every sequential copy, on the other hand, is naturally limited in terms of multi-generation and mass copying.

The advent of the recent popularity in the digital format has also brought about a slew of copy protection and digital rights management (DRM) systems and methods. These systems and methods use technologies such as encryption, watermarking and right descriptions (e.g. rules for accessing and copying data).

One way of protecting content in the form of digital data is to ensure that content will only be transferred between devices if:

- the receiving device has been authenticated as being a compliant device, and
- the user of the content has the right to transfer (move, copy) that content to another device.

If transfer of content is allowed, this will typically be performed in an encrypted way to make sure that the content cannot be captured illegally in a useful format.

Technology to perform device authentication and encrypted content transfer is available and is called a secure authenticated channel (SAC). Although it might be allowed to make copies of content over a SAC, the content industry is very bullish on content distribution over the Internet. This results in disagreement of the content industry on transferring content over interfaces that match well with the Internet, e.g. Ethernet.

Further, it should be possible for a user visiting his neighbor to watch a movie, which he owns, on the neighbor's big television screen. Typically, the content owner will disallow this, but it might become acceptable if it can be proved that a license holder of that movie (or a device that the license holder owns) is near that television screen.

It is therefore of interest to be able to include an authenticated distance measurement when deciding whether content should be accessed or copied by other devices.

In the article by Stefan Brands and David Chaum, "Distance-Bounding protocols", Eurocrypt '93 (1993), Pages 344-359, integration of distance-bounding protocols with public-key identification schemes is described. Here distance measurement is described based on time measurement using challenge and response bits and with the use of a commitment protocol. This does not allow authenticated device compliancy testing and is not efficient when two devices must also authenticate each other.

It is an object of the invention to obtain a solution to the problem of performing a secure transfer of content within a limited distance.

This is obtained by a method for a first communication device to performing authenticated distance measurement between the first communication device and a second communication device, wherein the first and the second communication device share a common secret and the common secret is used for performing the distance measurement between the first and the second communication device.

Because the common secret is being used for performing the distance measurement, it can be ensured that when measuring the distance from the first communication device to the second communication device, it is the distance between the right devices that is being measured.

The method combines a distance measurement protocol with an authentication protocol. This enables authenticated device compliancy testing and is efficient, because a secure channel is anyhow needed to enable secure communication between devices and a device can first be tested on compliancy before a distance measurement is executed.

In a specific embodiment, the authenticated distance measurement is performed according to the following steps;

- transmitting a first signal from the first communication device to the second communication device at a first time t**1**, the second communication device being adapted for receiving the first signal, generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal to the first device,
- receiving the second signal at a second time t**2**,
- checking if the second signal has been modified according to the common secret, and

- determining the distance between the first and the second communication device according to a time difference between t**1** and t**2**.

When measuring a distance by measuring the time difference between transmitting and receiving a signal and using a secret, shared between the first and the second communication device, for determining whether the returned signal really originated from the second communication device, the distance is measured in a secure authenticated way ensuring that the distance will not be measured to a third communication device (not knowing the secret). Using the shared secret for modifying the signal is a simple way to perform a secure authenticated distance measurement.

In a specific embodiment, the first signal is a spread spectrum signal. Thereby a high resolution is obtained and it is possible to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In another embodiment the step of checking if the second signal has been modified according to the common secret is performed by the steps of:

- generating a third signal by modifying the first signal according to the common secret, and
- comparing the third signal with the received second signal.

This method is an easy and simple way of performing the check, but it requires that both the first communication device and the second communication device know how the first signal is being modified using the common secret.

In a specific embodiment the first signal and the common secret are bit words and the second signal comprises information being generated by performing an exclusive OR operation (XOR) between the bit words. Thereby, it is a very simple operation that has to be performed, resulting in demand for few resources by both the first and the second communication device when performing the operation.

In an embodiment, the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of:

- performing an authentication check from the first communication device on the second communication device by checking whether the second communication device is compliant with a set of predefined compliance rules, and
- if the second communication device is compliant, sharing the common secret by transmitting the secret to the second communication device.

This is a secure way of performing the sharing of the secret, ensuring that only devices being compliant with compliance rules can receive the secret. Further, the shared secret can afterwards be used for generating a SAC channel between the two devices. The secret could be shared using e.g. key transport mechanisms as described in ISO 11770-3. Alternatively, a key agreement protocol could be used, which e.g. is also described in ISO 11770-3.

In another embodiment the authentication check further comprises checking if the identification of the second device is compliant with an expected identification. Thereby, it is ensured that the second device really is the device that it should be. The identity could be obtained by checking a certificate stored in the second device.

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between the first and the second communication device and checking whether the measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. By using the authenticated distance measurement in connection with sharing data between devices, unauthorized distribution of content can be reduced.

In a specific embodiment the data stored on the first device is sent to the second device if it is determined that the data stored on the first device are to be accessed by the second device.

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between a third communication device and the second communication device and checking whether the measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. In this embodiment, the distance is not measured between the first communication device, on which the data are stored, and the second communication device. Instead, the distance is measured between a third communication device and the second communication device, where the third communication device could be personal to the owner of the content.

The invention also relates to a communication device for performing authenticated distance measurement to a second communication device, where the communication device shares a common secret with the second communication device and where the communication device comprises means for measuring the distance to the second device using the common secret.

In an embodiment, the device comprises:

- means for transmitting a first signal to a second communication device at a first time t**1**, the second communication device being adapted for receiving the first signal, generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal,
- means for receiving the second signal at a second time t**2**,
- means for checking if the second signal has been modified according to the common secret, and
- means for determining the distance between the first and the second communication device according to a time difference between t**1** and t**2**.

The invention also relates to an apparatus for playing back multimedia content comprising a communication device according to the above.

In the following preferred embodiments of the invention will be described referring to the figures, wherein:

FIG. **1** illustrates authenticated distance measurement being used for content protection,

FIG. **2** is a flow diagram illustrating the method of performing authenticated distance measurement,

FIG. **3** illustrates in further detail the step of performing the authenticated distance measurement shown in FIG. **2**, and

FIG. **4** illustrates a communication device for performing authenticated distance measurement.

FIG. **1** illustrates an embodiment wherein the authenticated distance measurement is being used for content protection. In the center of the circle **101** a computer **103** is placed. The computer comprises content, such as data, software, images, multimedia content being video and/or audio, stored on e.g. a hard disk, solid state memory, a DVD or a CD. The owner of the computer **103** owns the content and therefore the computer is authorized to access and present the multimedia content for the user. When the user wants to make a legal copy of the content on another device via e.g. a SAC, the distance between the other device and the computer **103** is measured and only devices within a predefined distance illustrated by the devices **105**, **107**, **109**, **111**, **113** inside the circle **101** are allowed to receive the content. Whereas the devices **115**, **117**, **119** having a distance to the computer **103** being larger than the predefined distance are not allowed to receive the content.

In the example a device is a computer **103**, but it could e.g. also be a DVD drive, a CD drive or a Video display device, as long as the device comprises a communication device for performing the distance measurement.

In a specific example, the distance might not be measured between the computer **103**, on which the data are stored, and the other device, it could be determined between a third device (e.g. a device being personal to the owner of the content and which does not contain the data) and the other device.

In FIG. **2** a flow diagram illustrates the general idea of performing authenticated distance measurement between two devices, **201** and **203** each comprising communication devices for performing the authenticated distance measurement. In the example the first device **201** comprises content which the second device **203** has requested. The authenticated distance measurement then is as follows. In step **205** the first device **201** authenticates the second device **203**; this could comprise the steps of checking whether the second device **203** is a compliant device and might also comprise the step of checking whether the second device **203** really is the device identified to the first device **201**. Then in step **207**, the first device **201** exchanges a secret with the second device **203**, which e.g. could be performed by transmitting a random generated bit word to the second device **203**. The secret should be shared securely, e.g. according to some key management protocol as described in e.g. ISO 11770.

Then in step **209**, a signal for distance measurement is transmitted to the second device **203**; the second device modifies the received signal according to the secret and retransmits the modified signal back to the first device. The first device **201** measures the round trip time between the signal leaving and the signal returning and checks if the returned signal was modified according to the exchanged secret. The modification of the returned signal according to some secret will most likely be dependent on the transmission system and the signal used for distance measurement, i.e. it will be specific for each communication system (such as 1394, Ethernet, Bluetooth, IEEE 802.11, etc.).

The signal used for the distance measurement may be a normal data bit signal, but also special signals other than for data communication may be used. In an embodiment spread spectrum signals are used to be able to get high resolution and to be able to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In a specific example a direct sequence spread spectrum signal is used for distance measurement; this signal could be modified by XORing the chips (e.g. spreading code consisting of 127 chips) of the direct sequence code by the bits of the secret (e.g. secret consists also of 127 bits). Also, other mathematical operations similar to XOR could be used.

The authentication **205** and exchange of secret **207** could be performed using the protocols described in some known ISO standards e.g. ISO 9798 and ISO 11770. For example the first device **201** could authenticate the second device **203** according to the following communication scenario:

First device->Second device: R_B||Text 1
where R_B is a random number
Second device->First device: CertA||TokenAB

Where CertA is a certificate of A
TokenAB=R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2)
R_A is a random number
Indentifier B is an option
sS_A is a signature set by A using private key S_A

If TokenAB is replaced with the token as specified in ISO 11770-3 we at the same time can do secret key exchange. We can use this by substituting Text2 by:

Text2:=eP_B(A||K||Text2)||Text3
Where eP_B is encrypted with Public key B
A is identifier of A
K is a secret to be exchanged

In this case the second device **203** determines the key (i.e. has key control), this is also called a key transport protocol, but also a key agreement protocol could be used. This may be undesirable in which case it can be reversed, such that the first device determines the key. A secret key has now been exchanged according to step **207** in FIG. **2**. Again, the secret key could be exchanged by e.g. a key transport protocol or a key agreement protocol.

After the distance has been measured in a secure authenticated way as described above, content data can be sent between the first and the second device in step **211** in FIG. **2**.

FIG. **3** illustrates in further detail, the step of performing the authenticated distance measurement. As described above, the first device **301** and the second device **303** have exchanged a secret; the secret is stored in the memory **305** of the first device and the memory **307** of the second device. In order to perform the distance measurement, a signal is transmitted to the second device via a transmitter **305**. The second device receives the signal via a receiver **311**, and microprocessor **313** modifies the signal by using the locally stored secret. The signal is modified by the second device according to rules known by the first device **301** and transmitted back to the first device **301** via a transmitter **315**. The first device **301** receives the modified signal via a receiver **317** and in **319** the received modified signal is compared to a signal, which has been modified locally i.e. by the first device. The local modification is performed in microprocessor **321** by using the signal transmitted to the second device in transmitter **305** and then modifying the signal using the locally stored secret similar to the modification rules used by the second device. If the received modified signal and the locally modified signal are identical, then the received signal is authenticated and can be used for determining the distance between the first and the second device. If the two signals are not identical, then the received signal cannot be authenticated and can therefore not be used for measuring the distance as illustrated by **325**. In microprocessor **323** the distance is calculated between the first and the second device; this could e.g. be performed by measuring the time, when the signal is transmitted by the transmitter **309** from the first device to the second device and measuring when the receiver **317** receives the signal from the second device. The time difference between a transmittal time and a reception time can then be used for determining the physical distance between the first device and the second device.

In FIG. **4** a communication device for performing authenticated distance measurement is illustrated. The device **406** comprises a receiver **403** and a transmitter **411**. The device further comprises means for performing the steps described above, which could be performed by executing software using a microprocessor **413** connected to memory **415** via a communication bus **417**. The communication device could then be placed inside devices such as a DVD, a DVD recorder, a computer, a CD, a CD recorder, a solid state memory, a television and other devices for providing protected content, accessing protected content, or authorizing the access to protected content.

What is claimed is:

1. A first device for controlling delivery of protected content to a second device, the first device comprising:

a memory;

a processor, said processor arranged to:

receive a certificate of the second device, the certificate providing information regarding the second device;

determine whether the second device is compliant with a set of compliance rules utilizing said information provided in said certificate;

provide a first signal to the second device depending when the second device is determined to be compliant with the set of compliance rules;

receive a second signal from the second device after providing the first signal;

determine whether the second signal is derived from a secret known by the first device;

determine whether a time difference between providing the first signal and receiving the second signal is less than a predetermined time; and

allow the protected content to be provided to the second device when at least the second signal is determined to be derived from the secret and the time difference is less than the predetermined time.

2. The first device of claim **1**, wherein the first signal comprises a random number.

3. The first device of claim **1**, wherein the second signal is formed by modifying the first signal based on the secret, wherein the modification comprises performing an XOR operation on the first signal.

4. The first device of claim **1**, wherein the processor is further arranged to provide the secret to the second device.

5. The first device of claim **4**, wherein the secret is securely provided using one of: a key transport protocol, a key management protocol and a key agreement protocol.

6. The first device of claim **4**, wherein the processor arranged to provide the secret to the second device comprises the processor arranged to provide the secret to the second device via encryption by a public key of a private/public key-pair of the second device, if the second device is compliant, said secret comprising a random number.

7. The first device of claim **1**, wherein the processor is further arranged to receive the secret from the second device.

8. The first device of claim **7**, wherein the secret is securely received using one of: a key transport protocol, a key management protocol and a key agreement protocol.

9. The first device of claim **1**, wherein the processor arranged to determine whether the second signal is derived from the secret is arranged to:

modify the first signal according to the secret;

compare the modified first signal with the second signal; and

provide an indication when said modified first signal is identical to the second signal.

10. The first device of claim **1**, wherein the first signal and the secret are of comparable length.

11. The first device of claim **1**, wherein the processor is further arranged to determine an identity of the second device using the certificate.

12. The first device of claim **1**, wherein the certificate comprises a public key.

13. The first device of claim **1**, wherein the processor is further arranged to provide a certificate to the second device.

14. The first device of claim **1**, wherein the predetermined time is based on a communication system associated with the first device.

15. The first device of claim **1**, wherein the second signal comprises the first signal modified by the secret.

16. The first device of claim **1**, wherein the processor is further arranged to:

provide instruction to a third device to transmit said protected content, wherein said protected content is stored on said third device.

17. A system for controlling the transmission of protected content from a content provider to a requesting device, the content provider comprising:

means for receiving a certificate of the requesting device, the certificate providing information for validating the requesting device as being compliant with a set of compliancy rules;

means for validating that the requesting device is compliant with the set of compliancy rules using said information contained in said certificate;

means for transmitting a first signal to the requesting device at a first time when said requesting device is validated as being compliant with the set of compliancy rules;

means for receiving a second signal at a second time from the requesting device;

means for providing the protected content to the requesting device after determining the second signal depends on a secret known to the content provider, and

a time difference between the first time and the second time is less than a predetermined time.

18. The system of claim **17**, wherein said protected content is stored on a third device.

19. The system of claim **18**, wherein said means for providing the requested content comprises:

means for providing instruction to said third device to provide said content to said requesting device.

20. The system of claim **18**, wherein the third device is one of: a DVD, CD and a storage device.

21. The system of claim **17**, wherein the secret is securely received by the content provider.

22. The system of claim **17**, wherein the secret is securely transmitted by the content provider.

23. The system of claim **17**, wherein the certificate identifies the requesting device.

24. The system of claim **17**, wherein the predetermined time is based on a type of communication protocol between the requesting device and the content provider.

25. The system of claim **17**, wherein the content provider is one of: a DVD, CD and a storage device.

26. The system of claim **17**, wherein the second signal comprises the first signal modified by the secret.

27. A first device in communication with a second device, the first device comprising:

a memory;

a processor in communication with the memory, the processor arranged to execute software stored on the first device, the software configured to:

receive from the second device a request for a protected content and a certificate providing information associated with the second device;

determine whether the second device is suitable for receiving said protected content, wherein determining suitability of said second device is based on said information provided in said certificate;

- provide a first signal to said second device when said second device is determined to be suitable for receiving said protected content;
- receive from said second device a second signal;
- determine whether said second signal is representative of said first signal modified according to a secret known by said first device and said second device;
- determine whether a time difference between a time of providing the first signal and receiving the second signal is less than a predetermined time; and
- initiate transmission of said protected content to said second device when at least said second signal is representative of said first signal modified according to a secret known by said first device and said second device and said time difference is less than the predetermined time.

28. The first device of claim **27**, wherein said protected content is stored on said first device.

29. The first device of claim **27**, wherein the software configured to initiate said initiating transmission of said protected content is further configured to provide instruction to a third device to transmit said protected content, wherein said protected content is stored on said third device.

30. The first device of claim **29**, wherein said third device is one of a DVD, a CD and a storage device.

31. The first device of claim **29**, wherein said third device is remotely located from said first device.

32. The first device of claim **27**, wherein suitability is determined as being compliant with a set of compliancy rules.

33. The first device of claim **27**, wherein the software is further arranged to:

- provide the secret to the second device via encryption by a public key of a private/public key-pair of the second device, if the second device is suitable, said secret comprising a random number.

34. A method of a first device controlling delivery of protected content to a second device, the method comprising:

- receiving a certificate of the second device, the certificate providing information regarding the second device;
- determining whether the second device is compliant with a set of compliance rules utilizing said information provided in said certificate;
- providing a first signal to the second device depending when the second device is determined to be compliant with the set of compliance rules;
- receiving a second signal from the second device after providing the first signal;
- determining whether the second signal is derived from a secret known by the first device;
- determining whether a time difference between providing the first signal and receiving the second signal is less than a predetermined time; and
- allowing the protected content to be provided to the second device when at least the second signal is determined to be derived from the secret and the time difference is less than the predetermined time.

35. The method of claim **34**, wherein the first signal comprises a random number.

36. The method of claim **34**, wherein the second signal is formed by modifying the first signal based on the secret, wherein the modification comprises performing an XOR operation on the first signal.

37. The method of claim **34**, further comprising providing the secret to the second device.

38. The method of claim **37**, wherein the secret is securely provided using one of: a key transport protocol, a key management protocol and a key agreement protocol.

39. The method of claim **34**, further comprising receiving the secret from the second device.

40. The method of claim **39**, wherein the secret is securely received using one of: a key transport protocol, a key management protocol and a key agreement protocol.

41. The method of claim **34**, wherein the step of determining whether the second signal is derived from the secret comprises:

- modifying the first signal according to the secret;
- comparing the modified first signal with the second signal; and
- providing an indication when said modified first signal is identical to the second signal.

42. The method of claim **34**, wherein the first signal and the secret are of comparable length.

43. The method of claim **34**, further comprising determining an identity of the second device using the certificate.

44. The method of claim **34**, wherein the certificate comprises a public key.

45. The method of claim **34**, further comprising providing a certificate to the second device.

46. The method of claim **34**, wherein the predetermined time is based on a communication system associated with the first device.

47. The method of claim **34**, wherein the second signal comprises the first signal modified by the secret.

48. The method of claim **34**, further comprising providing instruction to a third device to transmit said protected content, wherein said protected content is stored on said third device.

49. A first device for controlling delivery of protected content to a second device, the first device comprising:

- a memory;
- a processor, the processor arranged to:
- receive a certificate from the second device prior to sending a first signal;
- determine from the certificate if the second device is compliant;
- provide a secret to the second device via encryption by a public key of a private/public key-pair of the second device, if the second device is compliant, said secret comprising a random number;
- provide the first signal to the second device;
- receive a second signal from the second device after providing the first signal;
  - determine if the second signal is derived from the secret by determining whether the second signal is the first signal modified based on the secret;
- determine whether a time difference between providing the first signal and receiving the second signal is less than a predetermined time; and
- allow the protected content to be provided to the second device at least when the second signal is determined to be derived from the secret and the time difference is less than the predetermined time.

50. The first device of claim **49**, wherein the processor is further arranged to:

- use the secret to generate a secure authenticated channel between the first device and the second device,
- use the secure authenticated channel to provide the protected content to the second device.

51. The first device of claim **49**, wherein the secret and the first signal are of comparable length.

52. The first device of claim **49**, wherein the modification is a XOR operation using the first signal.

53. The first device of claim **49**, wherein the processor, arranged to determine that the second signal is derived from the secret, is further arranged to:

modify the first signal according to the secret;

compare the modified first signal with the second signal; and

determine that the modified first signal is identical to the second signal.

54. The first device of claim **49**, wherein the first signal comprises a random number.

55. A method of a first device controlling delivery of protected content to a second device, the method comprising:

receiving a certificate from the second device prior to sending a first signal;

determining from the certificate if the second device is compliant;

providing a secret to the second device via encryption by a public key of a private/public key-pair of the second device, if the second device is compliant, said secret comprising a random number;

providing the first signal to the second device;

receiving a second signal from the second device after providing the first signal;

determining if the second signal is derived from the secret by determining whether the second signal is the first signal modified based on the secret;

determining whether a time difference between providing the first signal and receiving the second signal is less than a predetermined time; and

allowing the protected content to be provided to the second device at least when the second signal is determined to be derived from the secret and the time difference is less than the predetermined time.

56. The method of claim **55**, further comprising:

using the secret to generate a secure authenticated channel between the first device and the second device,

using the secure authenticated channel to provide the protected content to the second device.

57. The method of claim **55**, wherein the secret and the first signal have the same bit length.

58. The method of claim **55**, wherein the modification is a XOR operation using the first signal.

59. The method of claim **55**, wherein the step of determining that the second signal is derived from the secret comprises:

modifying the first signal according to the secret;

comparing the modified first signal with the second signal; and

determining that the modified first signal is identical to the second signal.

60. The method of claim **55**, wherein the first signal comprises a random number.

* * * * *

9

US006772114B1

(12) United States Patent
Sluijter et al.

(10) **Patent No.: US 6,772,114 B1**
(45) **Date of Patent: Aug. 3, 2004**

(54) **HIGH FREQUENCY AND LOW FREQUENCY AUDIO SIGNAL ENCODING AND DECODING SYSTEM**

(75) Inventors: **Robert Johannes Sluijter**, Eindhoven (NL); **Andreas Johannes Gerrits**, Eindhoven (NL); **Rakesh Taori**, Eindhoven (NL); **Samir Chennoukh**, Eindhoven (NL)

(73) Assignee: **Koninklijke Philips Electronics N.V.**, Eindhoven (NL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 455 days.

(21) Appl. No.: **09/710,916**

(22) Filed: **Nov. 13, 2000**

(30) **Foreign Application Priority Data**

Nov. 16, 1999 (EP) 99203819

(51) **Int. Cl.**^{7} **G10L 19/00**

(52) **U.S. Cl.** **704/220**; 704/262

(58) **Field of Search** 704/200, 200.1, 704/201, 205, 228, 261–269

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,581,652	A	*	12/1996	Abe et al.	704/222
5,710,863	A	*	1/1998	Chen	704/200.1
5,774,837	A		6/1998	Yeldener et al.	704/208
5,867,815	A	*	2/1999	Kondo et al.	704/228
6,078,880	A	*	6/2000	Zinser et al.	704/208
6,233,550	B1	*	5/2001	Gersho et al.	704/208

FOREIGN PATENT DOCUMENTS

EP	0648024 A1	12/1995	H04B/1/66

OTHER PUBLICATIONS

“A 13 KBIT/S Wideband Speech CODEC Based on SB–ACELP” J. Schnitzler, IEEE International Conference on Acoustics, Seattle Wa, vol. Conf. 23, May 12–15, 1998 p. 157–160.

“Hi–BIN: an Alternative Approach to Wideband Speech Coding” Taori et al, IEEE International Conference on Acoustics, Speech and Signal Processing, Istambul, Turkey, vol. 2, Jun. 5–9, 2000, p. 1157–1160.

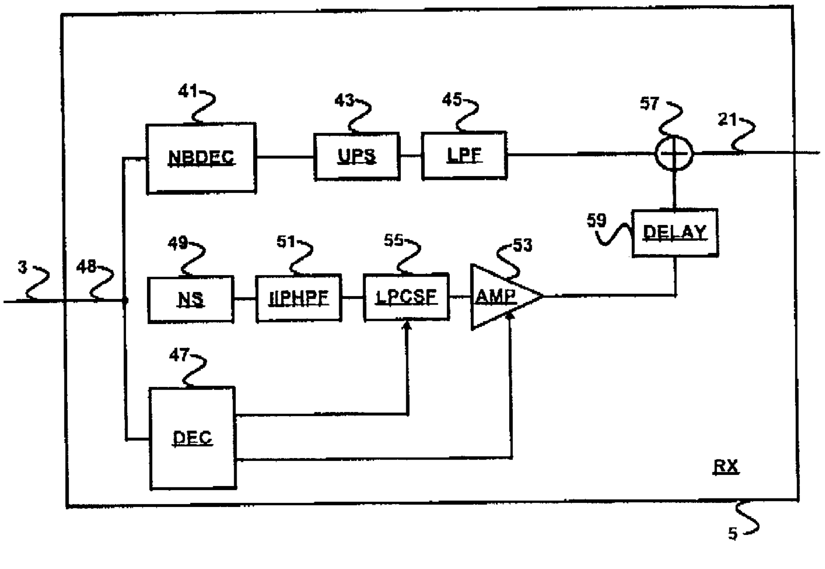
* cited by examiner

Primary Examiner—Richemond Dorvil
Assistant Examiner—Abulk Azad

(57) **ABSTRACT**

In an audio transmission system, an input signal is split up into two spectral portions in a transmitter. These spectral portions are coded by their own respective coder. The low-frequency signal portion is coded by a regular narrow-band coder and the high frequency portion is coded using a coder that outputs LPC codes and signal amplitude codes. In the receiver, the low frequency signal portion is reconstructed by a narrow-band decoder and the high frequency portion is reconstructed by applying a high pass filter to a white noise signal and applying an LPC filter that is controlled by the LPC codes to this filtered white noise signal and adjusting the signal amplitude with an amplifier that is controlled using the amplitude codes of the transmitter. The reconstructed low frequency signal and the reconstructed high frequency signal are then combined to yield a reconstructed output signal containing both frequency ranges.

21 Claims, 2 Drawing Sheets



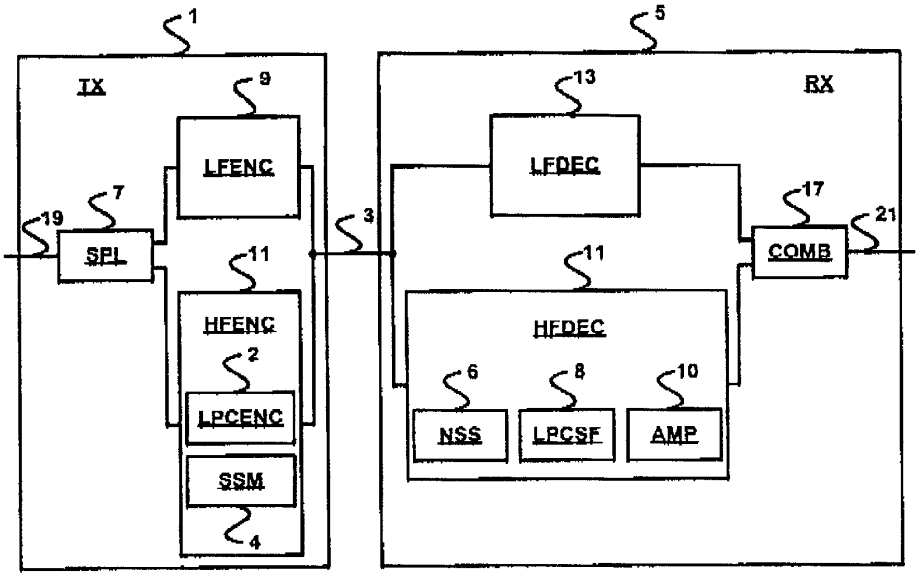

1
TX
9
LFENC
7
19
SPL
11
HFENC
2
LPCENC
SSM
4
3
5
13
RX
LFDEC
17
21
COMB
11
HFDEC
6
8
10
NSS
LPCSF
AMP

FIG. 1

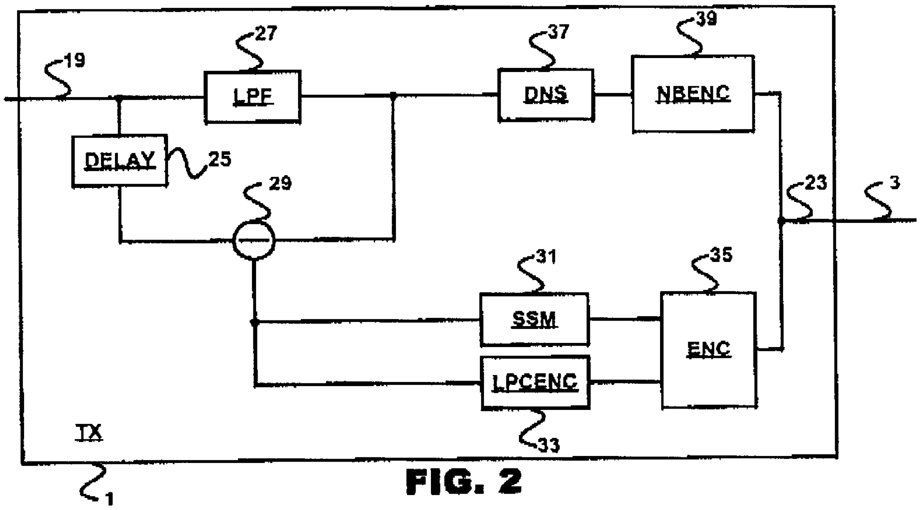

19
27
LPF
37
DNS
39
NBENC
DELAY
25
29
23
3
31
SSM
35
ENC
LPCENC
33
TX
1

FIG. 2

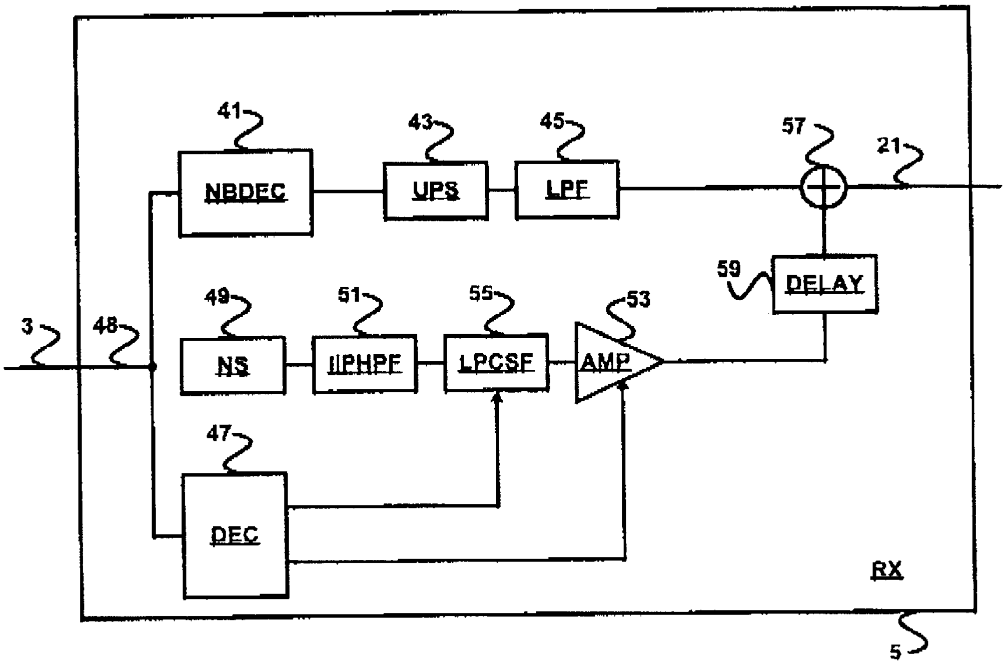

41
NBDEC
43
UPS
45
LPF
57
21
59
DELAY
3
48
49
NS
51
IIPHPF
55
LPCSF
53
AMP
47
DEC
RX
5

FIG. 3

HIGH FREQUENCY AND LOW FREQUENCY AUDIO SIGNAL ENCODING AND DECODING SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention relates to a transmission system employing a transmitter including a splitter for splitting up a transmission signal into a signal having a low frequency range and a signal having a high frequency range, and a first coding device for deriving a coded signal having a low frequency range from the signal having a low frequency range. The first coding device is arranged for transmitting the coded signal having a low frequency range to a receiver by a first transmission channel. The receiver employs a first decoder for forming a reconstructed signal having a low frequency range based on the coded signal having a low frequency range. The transmitter further employs a second coding device for deriving a coded signal having a high frequency range from the signal having a high frequency range, which second coding device is arranged for transmitting the coded signal having a high frequency range from the transmitter to the receiver by a second transmission channel. The receiver further employs a second decoder for forming a reconstructed signal having a high frequency range based on the coded signal having a high frequency range by using a noise signal coming from a noise signal source, and a combiner for combining the reconstructed signal having a low frequency range and the reconstructed signal having a high frequency range.

The invention further relates to a transmitter, a receiver, a coding device, a decoder, a coding method and a decoding method to be used in a transmission system of such type.

2. Description of the Relation Art

A prior art transmission system is known from EP 0 648 024 A1. This document describes a transmission system for audio signals in which the input signal is split up into spectral portions by a filter bank. These spectral portions are coded each by its own coding device, a sub-coder. In the sub-coder, the envelope of a signal is determined and this envelope is compared with a number of reference envelopes. An identification code of the reference envelope corresponding best to the envelope is transmitted to a receiver.

In the receiver, a decoder reconstructs a signal on the basis of the identification code, the envelope of which signal corresponds to the received reference envelope, after which the envelope is multiplied by a noise signal coming from a noise source, which results in a reconstructed spectral portion of the input signal. Subsequently, these reconstructed spectral portions are combined to thus form a reconstruction of the input signal.

A disadvantage of such a transmission system is that the coding device needs to have considerable computation capacity for the splitting up of the input signal into spectral portions by a filter bank in the transmitter and the combining of the spectral portions in the receiver with the aid of a combiner.

SUMMARY OF THE INVENTION

It is an object of the invention to provide a transmission system in which the necessary computation capacity is reduced.

For this purpose, the transmission system according to the invention is characterized in that a coding device comprises analysis means for determining prediction coefficients and for transmitting the prediction coefficients to a receiver and in that a decoding device is arranged for filtering the noise signal coming from the noise signal source during the reconstruction of the signal having a high frequency range by means of an LPC synthesis filter which is controlled by the prediction coefficients.

The input signal is split up into two portions, so that an optimum coding for each of the two frequency ranges can be selected. A first coding device utilizes a known coding, which is efficient for a signal having a low frequency range, at an associated efficient bit rate. A low-pass filler is sufficient for this signal. A second coding device utilizes the Linear Predicive Coding (LPC) to code the signal having a high frequency range in an efficient manner. Thanks to the properties of the LPC coding, a high-pass filter is sufficient and it is not necessary to apply down-sampling. Since the high-pass filter and the low-pass filter both require little computation capacity, and a down-sampler is omitted, the total required computation capacity is reduced.

The human auditory system in this high frequency range is considerably less precise, so that it is possible during the reconstruction of the signal having a high frequency range, to take a white noise source as a signal source and subsequently fitter the signal source with an LPC synthesis filter, so that a signal is obtained whose spectrum to the human auditory system sufficiently matches the original signal. Since it is avoided that the high frequency range is subdivided into smaller frequency ranges, which are to be processed separately, the required computation capacity is reduced.

An embodiment of the transmission system according to the invention is characterized in that the second coding device in the transmitter is arranged for generating an amplification code based on the signal having a high frequency range and in that the second decoder in the receiver is arranged for utilizing the amplification codes during the reconstruction of the signal having a high frequency range.

Since the coding device determines an amplification code by which the decoder subsequently amplifies the reconstructed signal, the number of prediction coefficients required is reduced, so that determining the prediction coefficients becomes simpler and requires less computation capacity.

The frequency ranges can be determined.

BRIEF DESCRIPTION Of THE DRAWINGS

The invention will be further described with reference to the Figures in which:

FIG. **1** shows a transmission system according to the invention,

FIG. **2** shows a transmitter according to the invention, and

FIG. **3** shows a receiver according to the invention.

DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED EMBODIMENT

FIG. **1** diagrammatically shows a transmission system according to the invention.

The input signal arrives through an input **19** of a transmitter ("TX") **1**. A splitter ("SPL") **7** splits up the input signal **19** into a signal that has a low frequency range and is processed by a first coder ("LFENC") **9**, and a signal that has a high frequency range and is processed by a second coder ("HFENC") **11**, the second coder **11** utilizing an LPC coder ("LPCENC") **2** and a signal strength meter ("SSM") **4**. The coder **11** is an LPC coder, which determines prediction coefficients of the signal that has a high frequency range. The coded signals appear on the output of the first coder **9** and the second coder **11** and are transmitted to a receiver ("RX") **5** by a transmission channel **3**. In this receiver **5**, the coded signal having a low frequency range is processed by a first decoder ("LFDEC") **13** and the coded signal having a high frequency range is processed by a second decoder ("HFDEC") **15**, while use is made of a noise signal source ("NSS") **6**, an LPC synthesis filter ("LPCSF") **8** and an amplifier ("AMP") **10**. The decoded signal having a low frequency range and the decoded signal having a high frequency range are then combined by a combiner ("COMB") **17** to an output signal that is rendered available on an output **21** of the receiver **5**.

FIG. **2** shows an embodiment of transmitter **1** (FIG. **1**) according to the invention.

The input signal arrives through the input **19** of transmitter **1**. The input signal is split up into two spectral portions, the signal having a low frequency range being the result of the processing of the input signal with the low-pass filter ("LPF") **27**, and the signal having a high frequency range being the result of determining the difference between the signal having a low frequency range coming from the low-pass filter **27** and the input signal delayed by a delay element ("DELAY") **25**. The difference signal is determined by the subtracter **29**. It is important for the low-pass filter **27** to have a linear phase characteristic. This may be achieved, for example, by using a finite impulse response filter having a length of **81** as a low-pass filter, so that the filtered signal is delayed by 40 samples. For speech may be chosen a passband frequency range between 0 and 3.4 kHz and a stop band from 4 to 8 kHz. The delay element **25** is used for compensating for the delay that occurs in the finite impulse response filter, so that the signals available at the subtracter **29** have the right phase relation.

The difference signal is then applied to a signal strength meter ("SSM") **31**, which measures the signal strength of the difference signal and generates amplification codes in response thereto. The signal strength is determined for sub-frames having a length from 0.5 . . . 10 ms of the signal having a high frequency range.

By means of a Hamming window h, the signal strength is determined based on the following equation [1]:

$$p_1 = \frac{1}{80}\sum_{n=0}^{79} h[n]s^2[n] \qquad [1]$$

where s is a 5 ms sub-frame and i the position in the frame. Four signal strengths are computed within one frame, thus i=1, 2, 3, 4.

For quantization purposes, the four signal strengths are converted to a logarithmic domain in accordance with the following equation [2]:

$$l_i=10\ \log_{10}\mathrm{p}_i \text{ where } i=1,2,3,4. \qquad [2]$$

The first signal strength l_1 is quantized with four bits, whereas the lust three signal strengths l_2 to l_4 are quantized differentially relative to the previously quantized signal strength with three bits.

The value of l_1 may be limited to a fixed range, for example, a range from −10 to 60 dB for 16-bit signals and is then quantized with 4 bits, which results in a quantized signal strength $\hat{l}_i$ and an index I_{l_i}. The remaining signal strengths are quantized differentially in accordance with the following equation [3]:

$$\Delta_i=l_i-\hat{l}_{i-}1 \qquad [3]$$

This differential quantization Δ_i may be limited to a range from, for example, −6 dBm to +6 dBm. The index representing this differential quantization is I_{l_i}. The quantized signal strength $\hat{l}_i$ is to be determined in accordance with the following equation [4] to be able to compute Δ_{i+1}:

$$\hat{l}_i=\hat{l}_{i-1}+\hat{\Delta}_i \qquad [4]$$

The amplification codes comprise the indices I_{l_i}.

The decoder determines the quantized signal strengths in the same manner.

The difference signal is also applied to an LPC coder ("LPCENC") **33**, which determines the prediction codes of the difference signal with the aid of an LPC analysis. The low frequency range in the difference signal is absent, so that down-sampling of the signal is not necessary. When the signal having a high frequency range is reconstructed by an LPC synthesis filter, a frequency characteristic having a sufficiently low amplitude level arises of its own accord in the low frequency range. With the aid of a sixth-order LPC analysis, the six LPC coefficients can be determined of a 15 ms segment of the signal having a high frequency range. For determining these six LPC coefficients, the average value of the segment is determined and subtracted from the samples in the segment, after which a 240-dot Hamming window function is applied. Subsequently, the Levinson-Durbin recursion is applied to the autocorrelation function of the windowed signal. To avoid sharp resonances, bandwidth expansion is used for which an expansion factor of 0.98 can be used.

The six LPC coefficients are converted to Line Spectral Frequencies (LSF) ω[n] (n=0,1,2 . . . ,5) in preparation for vector quantization. The quantized LSFs are based on their sensitivity to quantization errors. The sensitivity increases as the distance between neighboring LSFs decreases.

This is used by utilizing a weighing function Φ in accordance with the following equation [5]:

$$\Phi[n] = \begin{cases} \dfrac{1}{\omega[1]-\omega[0]} & \text{If } n=0 \\ \dfrac{1}{\omega[5]-\omega[4]} & \text{if } n=5 \\ \dfrac{1}{\min(\omega[n]-\omega[n-1],\ \omega[n+1])} & \text{if } 1 \le n \le 4 \end{cases} \qquad [5]$$

A single codebook c comprising 1024 predefined 6^{th}-order LSF vectors is used for the vector quantizer, the LSF vectors being obtained by training the codebook c with the LBG algorithm.

For each element j of the codebook c the following distance function is evaluated in accordance with the following equation [6]:

$$D_j = \sum_{n=0}^{5} \Phi[n]\cdot(\omega[n]-c_l[n])^2 \qquad [6]$$

The index of the codebook element having the shortest distance is selected. This LSF codebook index is sent to the decoder.

The signal having a low frequency range coming from the low-pass filter **27** is down-sampled by a down-sampler ("DNS") **37** and applied to a narrow-band coder ("NBENC")**39**. This narrow-band coder **39** is a normal coder optimized for a signal having a low frequency range as described, for example, in ITU G.729 or G.728. The type or operation of this narrow-band coder **39** is unimportant to the implementation of the invention. The narrow-band coder **39** generates coded signals that, together with the amplification codes coming from the signal strength meter **31** and the coded signals coming from the LPC coder **33** via coder ("ENC") **35**, are available on an output **23** of the transmitter **1** for further processing.

FIG. **3** shows an embodiment of receiver **5** (FIG. **1**) according to the invention.

The coded signals arriving through an input **48** of the transmission channel are applied to a narrow-band decoder ("NODEC") **41** and a decoder ("DEC") **47**, while each decoder processes the coded signals and amplification codes intended for it.

By the narrow-band coder **41**, a reconstructed signal having a low frequency range is recovered from the coded signal having a low frequency range after which up-sampling takes place by an up-sampler ("UPS") **43**. To avoid undesired signals in the high frequency range, which may be developed during decoding or up-sampling, the reconstructed signal, after up-sampling, is filtered by a low-pass filter ("LPF") **45**, which has a frequency characteristic that can be compared with the low-pass filter **27** in the transmitter.

The coded signal having a high frequency range and the amplification codes are convened by a decoder **47** into control signals for an LPC synthesis filter ("LPCSF") **55** and for an amplifier ("AMP") **53** by which the frequency characteristic and signal strength of the reconstructed signal can be adapted.

A noise source ("NS") **49** produces a white noise signal. The white noise signal includes noise segments of 80 samples in length, which are generated by a random pulse generator having a uniform random pulse distribution. This noise signal is processed by a sixth-order Infinite Impulse Response high-pass filter ("IIRHPF") **51** that has a 3500 Hz cut-off frequency, so that a filtered noise signal arises which has a frequency range that is comparable to the frequency range of the signal having a high frequency range.

The amplitude spectrum of the filtered noise signal coming from the high-pass filter **51** is adapted by an LPC synthesis filter **55** to the amplitude spectrum of the signal having a high frequency range. The LPC parameters necessary for setting the LPC synthesis filter **55** are obtained by selecting the right LSFs from the codebook with the aid of a received LPC codebook index and converting these LSFs into LPC parameters.

During the reconstruction of the signal having a high frequency range by an LPC synthesis filter, an amplitude spectrum having a sufficiently low amplitude level will arise of its own accord in the low frequency range.

The filtered noise signal coming from the LPC synthesis filter **55** is amplified by the amplifier **53**, which is set to the indices in the received amplification codes. This achieves that the signal strength of the reconstructed signal having a high frequency range is adapted to the signal strength of the signal having a high frequency range. The signal strength is indicated in the amplification code by the received indices I_{l_i} (i=1, . . . ,4). The indices are decoded and then converted from the logarithmic domain to the linear domain:

$$\hat{p}_l = 10^{\frac{\bar{I}_l}{10}}$$

The filtered noise signal is subdivided into 5 ms sub-frames. Per sub-frame s', the signal strength is determined by the following equation [7]:

$$p'_l = \frac{1}{80}\sum_{n=0}^{79} h[n]\cdot s'^2[n] \qquad [7]$$

where h is a Hamming window.

The scale factor g_l for the sub-frame I is determined in accordance with the following equation [8]:

$$g_l = \sqrt{\frac{\hat{p}_f}{p'_l}} \qquad [8]$$

The segments of the noise signal are scaled, that is to say, amplified by a factor g_l and, with an overlap, combined to form the high frequency reconstructed signal.

Since it is possible for various signal delays to arise during the reconstruction of the signal having a high frequency range and the signal having a low frequency range, a delay element ("DELAY") **59** is provided for delaying the signal coming from the amplifier **53**. In the case where the signal having a low frequency range experiences less delay than the signal having a high frequency range, the delay element **59** may be inserted between the low-pass filter **45** and the combiner **57**.

The reconstructed signal having a low frequency range coming from the low-pass filter **45**, and the reconstructed signal having a high frequency range coming from the delay element **59** are combined by a combiner **57** to an output signal that is rendered available on an output **21** of the receiver. Since the frequency characteristic of the reconstructed signal having a low frequency range and the reconstructed signal having a high frequency range shows little overlap, the output signal having a complete frequency range can be obtained by simply adding up the two reconstructed signals.

While the embodiments of the invention disclosed herein are presently considered to be preferred, various changes and modifications can be made without departing from the spirit and scope of the invention. The scope of the invention is indicated in the appended claims, and all changes that come within the meaning and range of equivalents are intended to be embraced therein.

What is claimed is:

1. A transmission system, comprising:

a transmitter including

a splitter for splitting up a transmission signal into a low frequency signal within a low frequency range and a high frequency signal within a high frequency range, the low frequency range being lower than the high frequency range,

wherein said splitter applies a low-pass filter to the transmission signal to generate the low frequency signal,

wherein said splitter applies a delay to the transmission signal to generate a delayed transmission signal, and

wherein said splitter determines a difference between the low frequency signal and the delayed transmission signal to generate the high frequency signal,

a first coder for deriving a first coded signal within the first frequency range from the low frequency signal, and

a second coder for deriving a second coded signal within the high frequency range from the high frequency signal;

a receiver in electrical communication with said transmitter to receive the first coded signal and the second coded signal, said receiver including

a first decoder for forming a first reconstructed signal within the first frequency range based on the first coded signal, and

a second decoder for forming a second reconstructed signal within the second frequency range based on the second coded signal and a noise signal.

2. The transmission system of claim **1**,

wherein said first coder sequentially applies a down-sampler and a narrow-band coder to generate the first coded signal.

3. The transmission system of claim **1**,

wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code;

wherein said second coder determines prediction coefficients based on the high frequency signal; and

wherein the second coded signal codes the amplification code and the prediction coefficients as components of the second coded signal.

4. The transmission system of claim **2**,

wherein the first decoder sequentially applies a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate the first reconstructed signal.

5. The transmission system of claim **2**,

wherein, based on the second coded signal, the second decoder sequentially applies a high-pass filter, a LPC synthesis filter and an amplifier to the noise signal to generate the second reconstructed signal.

6. The transmission system of claim **5**,

wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code;

wherein said second coder codes the amplification code as one component of the second coded signal; and

wherein said second decoder uses the amplification code to set said amplifier.

7. The transmission system of claim **5**,

wherein said second coder determines prediction coefficients based on the high frequency signal;

wherein said second coder codes the prediction coefficients as one component of the second coded signal, and

wherein said second decoder uses the prediction coefficients to control said LPC synthesis filter.

8. The transmission system of claim **2**, further comprising:

a combiner for combining the first reconstructed signal and the second reconstructed signal.

9. The transmission system of claim **8**,

wherein said receiver applies a delay to one of the first reconstructed signal and the second reconstructed signal prior to said combiner combining the first reconstructed signal and the second reconstructed signal.

10. A transmission system, comprising:

a transmitter including

a splitter for splitting up a transmission signal into a low frequency signal within a low frequency range and a high frequency signal within a high frequency range, the low frequency range being lower than the high frequency range,

a first coder for deriving a first coded signal within the first frequency range from the low frequency signal, and

a second coder for deriving a second coded signal within the high frequency range from the high frequency signal;

a receiver in electrical communication with said transmitter to receive the first coded signal and the second coded signal, said receiver including

a first decoder for sequentially applying a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate a first reconstructed signal within the first frequency range, and

a second decoder, wherein, based on the second coded signal, said second decoder sequentially applies a high-pass filter, a LPC synthesis filter and an amplifier to a noise signal to generate the second reconstructed signal.

11. The transmission system of claim **10**,

wherein said first coder sequentially applies a down-sampler and a narrow-band coder to generate the first coded signal.

12. The transmission system of claim **10**,

wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code;

wherein said second coder determines prediction coefficients based on the high frequency signal; and

wherein the second coded signal codes the amplification code and the prediction coefficients as components of the second coded signal.

13. The transmission system of claim **10**,

wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code;

wherein said second coder codes the amplification code as one component of the second coded signal; and

wherein said second decoder uses the amplification code to set said amplifier.

14. The transmission system of claim **10**,

wherein said second coder determines prediction coefficients based on the high frequency signal;

wherein said second coder codes the prediction coefficients as one component of the second coded signal, and

wherein said second decoder uses the prediction coefficients to control said LPC synthesis filter.

15. The transmission system of claim **10**, further comprising:

a combiner for combining the first reconstructed signal and the second reconstructed signal.

16. The transmission system of claim **15**,

wherein said receiver applies a delay to one of the first reconstructed signal and the second reconstructed signal prior to said combiner combining the first reconstructed signal and the second reconstructed signal.

17. A transmitter, comprising:

a splitter for splitting up a transmission signal into a low frequency signal within a low frequency range and a high frequency signal within a high frequency range, the low frequency range being lower than the high frequency range,

wherein said splitter applies a low-pass filter to the transmission signal to generate the low frequency signal,

wherein said splitter applies a delay to the transmission signal to generate a delayed transmission signal, and

wherein said splitter determines a difference between the low frequency signal and the delayed transmission signal to generate the high frequency signal;

a first coder for deriving a first coded signal within the first frequency range from the low frequency signal; and

a second coder for deriving a second coded signal within the high frequency range from the high frequency signal.

18. The transmitter of claim **17**,

wherein said first coder sequentially applies a down-sampler and a narrow-band coder to generate the first coded signal.

19. The transmission system of claim **17**,

wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code;

wherein said second coder determines prediction coefficients based on the high frequency signal; and

wherein the second coded signal codes the amplification code and the prediction coefficients as components of the second coded signal.

20. A receiver, comprising:

a first decoder receiving a first coded signal with a low frequency range, said first decoder for sequentially applying a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate a first reconstructed signal within the low frequency range;

a second decoder receiving a second coded signal within a high frequency range that is higher the low frequency range

wherein, based on the second coded signal, said second decoder sequentially applies a high-pass filter, a LPC synthesis filter and an amplifier to a noise signal to generate a second reconstructed signal within the high frequency range; and

a combiner for combining the first reconstructed signal and the second reconstructed signal.

21. The receiver of claim **20**,

wherein said receiver applies a delay to one of the first reconstructed signal and the second reconstructed signal prior to said combiner combining the first reconstructed signal and the second reconstructed signal.

* * * * *

10

US00RE43564E

(19) **United States**
(12) **Reissued Patent**
Van Ee

(10) **Patent Number: US RE43,564 E**
(45) **Date of Reissued Patent: Aug. 7, 2012**

(54) **HAND-HELD WITH AUTO-ZOOM FOR GRAPHICAL DISPLAY OF WEB PAGE**

(75) Inventor: **Jan Van Ee**, Irvine, CA (US)

(73) Assignee: **Koninklijke Philips Electronics N.V.**, Eindhoven (NL)

(21) Appl. No.: **12/980,454**

(22) Filed: **Dec. 29, 2010**

Related U.S. Patent Documents

Reissue of:
(64) Patent No.: **6,466,203**
Issued: **Oct. 15, 2002**
Appl. No.: **09/619,426**
Filed: **Jul. 19, 2000**

U.S. Applications:
(63) Continuation-in-part of application No. 09/062,364, filed on Apr. 17, 1998, now Pat. No. 6,211,856.

(51) **Int. Cl.**
G09G 5/00 (2006.01)

(52) **U.S. Cl.** **345/173**; 715/835

(58) **Field of Classification Search** 345/156–179; 715/835

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,746,981	A	5/1988	Nadan et al.
4,751,507	A	6/1988	Hama et al.
5,001,697	A	3/1991	Torres
5,063,535	A	11/1991	Jacobs et al.
5,119,079	A	6/1992	Hube et al.
5,406,307	A	4/1995	Hirayama et al.
5,463,725	A	10/1995	Henckel et al.
5,491,495	A	2/1996	Ward et al.
5,565,888	A	10/1996	Selker
5,596,346	A	1/1997	Leone et al.
5,726,883	A	3/1998	Levine et al.
5,739,744	A	4/1998	Roca et al.
5,854,624	A	12/1998	Grant
5,886,697	A	3/1999	Naughton et al.
5,956,025	A	9/1999	Goulden et al.
5,969,706	A	10/1999	Tanimoto et al.
5,973,691	A	10/1999	Servan-Schreiber
5,986,657	A	11/1999	Berteig et al.

(Continued)

FOREIGN PATENT DOCUMENTS

EP	0542660	A1	5/1993

(Continued)

OTHER PUBLICATIONS

Perlin et al: "Nested User Interface Components"; Proceedings of the 12th Annual ACM Syposium on User Interface Software and Technology, UIST'99, ACM 1999, pp. 1-8.

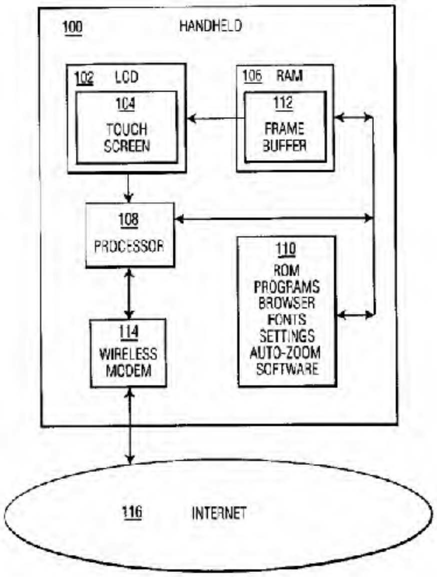
(Continued)

Primary Examiner — Nitin Patel
Assistant Examiner — Mansour M Said

(57) **ABSTRACT**

A mobile phone has a display with a touch screen. The device has a browser and is capable of retrieving a Web page from the Internet. The page is first displayed in its entirety. The user can recognize the page's general lay-out and presence of hyperlinks. When the user touches a particular location on the touch screen that corresponds to a portion of the page's image, the portion gets displayed so as to fill the display's area. Thus, the user can browse the Web with a display of limited size.

7 Claims, 2 Drawing Sheets



U.S. PATENT DOCUMENTS

6,073,036	A *	6/2000	Heikkinen et al.	455/550.1
6,104,334	A *	8/2000	Allport	341/175
6,211,856	B1	4/2001	Choi et al.	
2001/0013897	A1	8/2001	Kowno et al.	

FOREIGN PATENT DOCUMENTS

JP	10049305	A1	2/1998
WO	9954807	A1	10/1999

OTHER PUBLICATIONS

Smith et al: "Generalized and Stationary Scrolling"; UIST'99, CHI Letters, vol. 1, 1999, pp. 1-9.

Vander Zanden et al: Proceedings of the 12th Annual ACM Symposium on User Interface Software and Technology, Asheville, North Carolina, Nov. 7-10, 1999, ACM 1999.

* cited by examiner

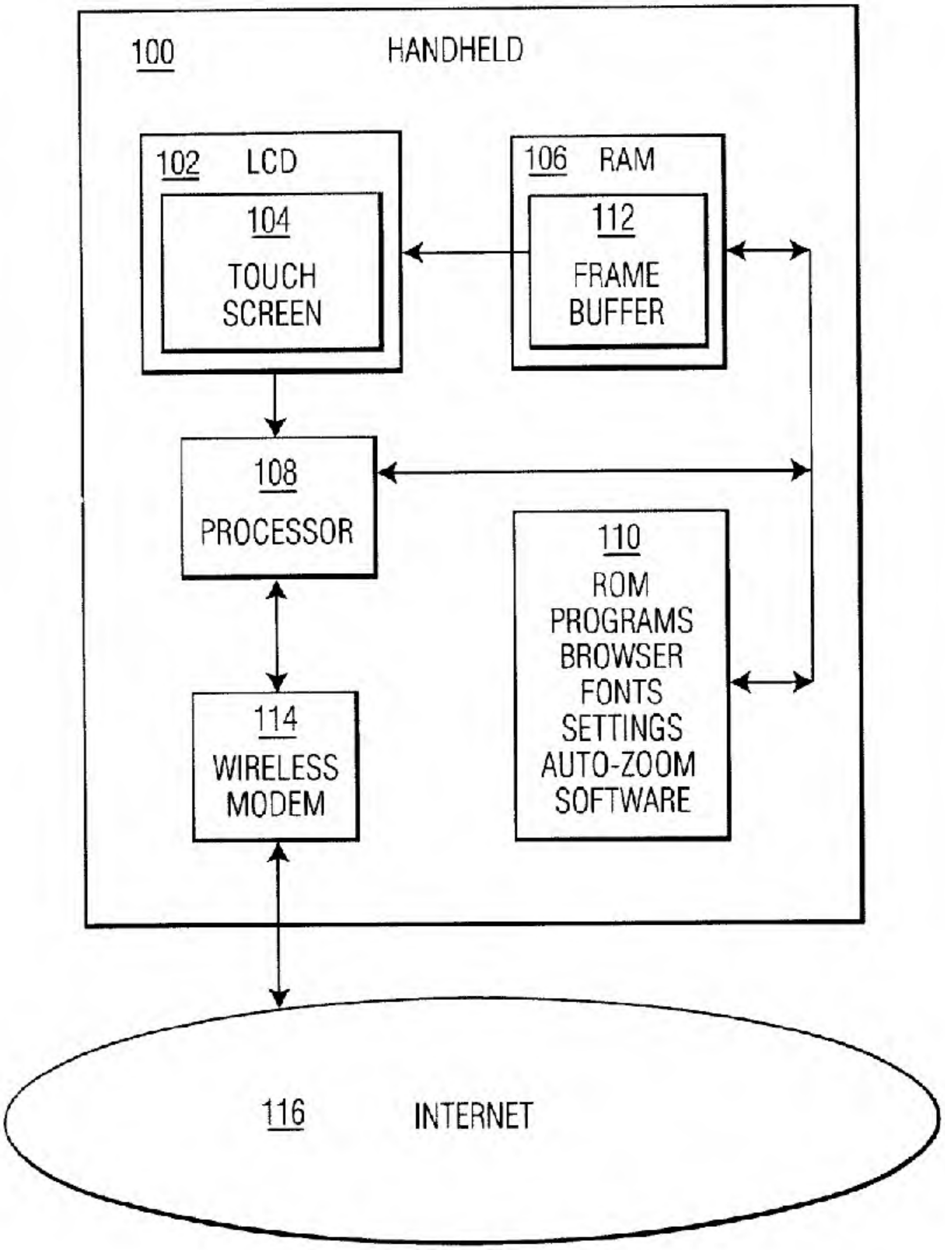

100
HANDHELD
102 LCD
104
TOUCH SCREEN
106 RAM
112
FRAME BUFFER
108
PROCESSOR
110
ROM
PROGRAMS
BROWSER
FONTS
SETTINGS
AUTO-ZOOM
SOFTWARE
114
WIRELESS MODEM
116 INTERNET

FIG. 1

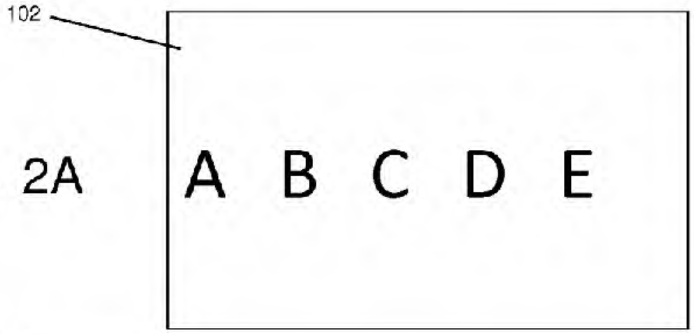


FIG. 2A

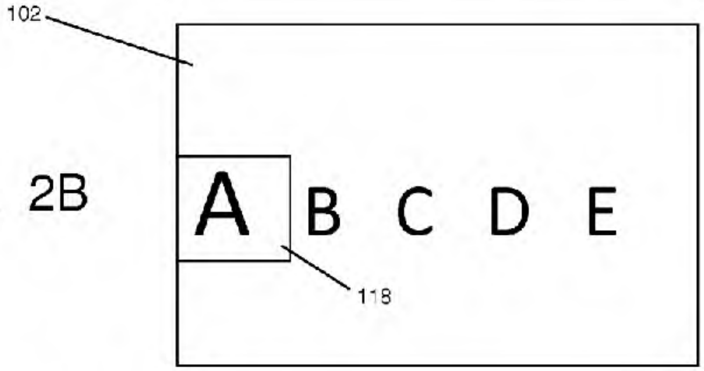


FIG. 2B

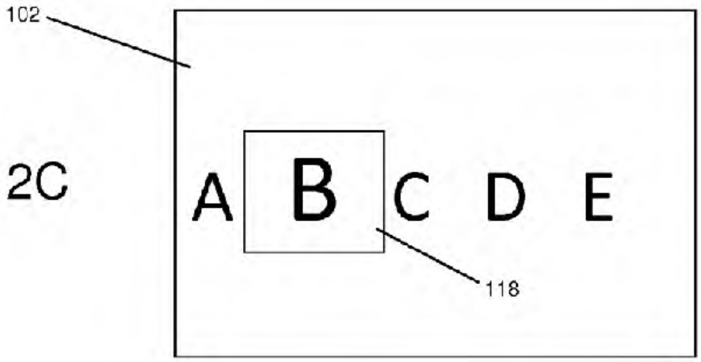


FIG. 2C

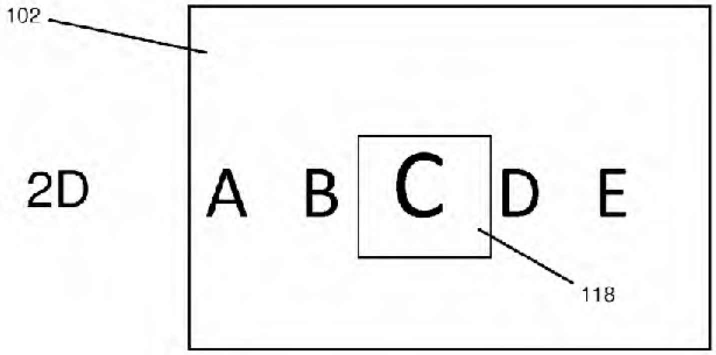


FIG. 2D

HAND-HELD WITH AUTO-ZOOM FOR GRAPHICAL DISPLAY OF WEB PAGE

Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.

RELATED APPLICATION

This application is a continuation-in-part under 37 C.F.R. §1.53(b).2 of co-pending U.S. Ser. No. 09/062,364 filed Apr. 17, 1198 *now U.S. Pat. No. 6,211,856* for Sung Choi and Jan van Ee for GRAPHICAL USER INTERFACE TOUCH SCREEN WITH AUTO ZOOM FEATURE.

FIELD OF THE INVENTION

The invention relates to graphical user interfaces (GUI), in particular to GUI's for devices with a relatively small screen real estate, such as handheld information appliances (palmtops. mobile phones. Web pads, PDA's or notebook computers, etc.)

BACKGROUND ART

Current trends indicate that by 2002 there will be 1B subscribers worldwide to mobile phones. By 2004 there will be more Mobile phones in use than PC's. Mobile phones have become personal, trusted devices. Mobile phones, such a the Genie manufactured by Philips Electronics, typically have an LCD as part of the user interface and there is a trend to provide an ever larger number of onboard software services.

Hand-held computing devices, such as personal digital assistants (PDA), e.g., the PalmIIIx manufactured by 3COM or a Windows CE-based handheld, can be connected to the Internet via a wireless modem. As a result, ubiquitous information access via the Internet has started to become reality. Examples of a wireless modems are, for example, the Minstrel marketed by Novatel Wireless, and the Ricochet from Metricom. The Minstrel is a two-way wireless modem for a PDA that lets the user browse the Web and receive email, among other things. In a more general sense, a wireless modem like the Minstrel or Ricochet provides the handheld device with an IP address that can be used by any type of application that uses the Internet for communication (within limitations of throughput, latency and coverage). The Minstrel uses a technology referred to as Cellular Digital Packet Data (CDPD) that is supported by the cellular service providers. Web surfing is limited to a CDPD speed cap of 19.2-kbps. The Ricochet has a faster connect rate, in the 28.8K-bps range, but it is supported in only three metropolitan centers (the San Francisco Bay area, Seattle and Wash.).

Studies further indicate that the functionalities of PDA's and mobile phones have started to converge, and that a mobile information society is developing. There will be an emerging of dedicated devices. PDA's are now work-related. In the near future PDA's will be personalized computers that stay with the user all the time. PDA's will get more power and smaller size and accommodate more, and more versatile, functionalities.

Bandwidth and display size are believed to be the factors that limit the usability and practicality of the handheld device, be it a mobile phone, a palmtop or a hybrid. In particular, the GUI and the services accessible to such handhelds are critical factors for the consumers' acceptability of such services. In particular, e-commerce or electronic shopping may benefit from the ubiquity of handhelds if the implementing technology addresses the consumers' needs in terms of user-friendliness of the handheld devices.

SUMMARY OF THE INVENTION

Co-pending U.S. Ser. No. 09/062,364 (PHA 23,387) mentioned above and incorporated herein by reference, corresponds to published International Application WO9954807. This document relates to a graphical user interface touch screen for displaying controllable functions of an electronic device. The function is displayed as an icon and at a scale size in which the function is recognizable by a user but too small to easily access features of the function. A magnified version of at least an area of the icon is provided upon the user touching the area of the icon. For example, the device has a Virtual alphanumeric keyboard. The softkeys displayed are too small for the user to select an individual one of them. Now, when the user touches the keyboard in a specific section that accommodates the desired key, the device's GUI magnifies that specific section so that the intended key re-appears at a larger scale and can be selected.

The inventor has realized that this feature, referred to as "auto-zoom", is not only useful within the context of a user-interface for control functionalities represented graphically by icons. The auto-zoom is also relevant to the rendering of any kind of graphical information on a display too small for the total information content, given the display's resolution and size. For example, handheld information processing devices with Internet access (browsers) and displays, such as PDA's, palmtops, web pads, mobile phones using, e.g., the WAP (wireless application protocol) technology, etc., can be given browsers for retrieving and navigating web pages from the Internet, but they cannot render a page in its entirety without losing information. The lay-out and general appearance of the image of the page, however, indicate whether portions may or may not be of interest to the user, e.g., as containing hyperlinks.

Such handheld devices provided with the auto-zoom feature let the user retrieve graphical information, e.g., a web page or streamed video that is stored, e.g., as a bitmap, in the display's framebuffer or another cache.

Accordingly, the invention relates to an information processing apparatus that has an input for receiving data from an external resource, e.g. the Internet, a display, and a data processing system. The system is connected to the input and to the display. The system processes the data upon receipt and renders on the display an image corresponding to the data received. The apparatus has a touch screen for enabling a user to interact with the apparatus. The system is operative to enable the user to select via the touch screen a portion of the image when displayed at a first scale. Upon the portion being selected the system renders the selected portion on the display at a second scale larger than the first scale (zoom-in). The portion selected corresponds to a location on the touch screen. The invention thus allows the user to perceive the graphical information of the image regardless of the display size. The invention is especially interesting to handhelds, such as PDA's, palmtops,. mobile phones, web pads (thin clients with browsing capabilities), etc., because the size of a handheld's display is necessarily small due to the required form factor and weight limitation. The ubiquitous information access via a browser is a great asset for Internet-enabled handhelds (comprising a wireless modem), as not only text pages but also, e.g., still pictures (e.g., jpeg), streaming video, web page with hyperlinks (e.g., HTML) and java animation are now within reach of these devices whose screen real estate needs not be the limiting factor anymore.

The apparatus in the invention can have one or more zoom levels.

The term "texting" is currently being used to refer to the sending and receiving of short text messages using mobile phones. Many service providers allow users to key in and send short text messages (SMS: short messaging service). Teenagers in Europe and East Asia seem to have embraced this technology, just as young people in the U.S. have gone for live chat and instant messaging on the Internet. The invention in U.S. Ser. No. 09/062,364 (PHA 23,387) improves the user-friendliness of the mobile phone's GUI. The invention of the auto-zoom extended to cover the rendering of arbitrary graphical information further broadens the scope of applicability of data processing handhelds, especially in the field of consumer electronics (CE).

Screenphones may also benefit from the current invention. A screenphone is typically a wired terminal that has a small display monitor and a keyboard. The Internet screenphone market is expanding rapidly. Analysts predict revenues in this market segment as over S2 B by 2002. The success of the Minitel system in France has triggered the introduction of screenphones elsewhere by banks to promote home banking and shopping.

BRIEF DESCRIPTION OF THE [DRAWING] *DRAWINGS*

The invention is explained below in further detail, by way of example and with reference to the accompanying [drawing with] *drawings, in which:*

FIG. 1 is a block diagram of a handheld device in the invention*; and*

FIGS. 2A-2D show a display of the handheld device illustrating the scrolling of a window at a second scale.

DETAILED EMBODIMENTS

As specified above, the invention relates to, among other things, extending the autozoom keyboard idea in U.S. Ser. No. 09/062,364 to any kind of graphical or displayable information, when the information cannot be displayed in its entirety. For example, displaying a web page with hyperlinks on a mobile phone, which has a small LCD with touch screen functionality, may render the user-interaction with the links cumbersome if possible at all, due to their size. The LCD can nevertheless display the web page in its entirety by scaling it down. This initial rendering upon retrieval of the page from the Internet may very well cause the page illegible. However, proper filtering of the scaled down image ensures that the user can still recognize screen areas of potential interest and the hyperlinks therein. When the user touches the screen, the portion of the image underneath the touched location is enlarged and displayed so that hyperlinks can be individually be selected, possibly after a next, similar zoom-in process.

FIG. 1 is a block diagram with main components of an apparatus **100** in the invention. Apparatus **100** is, for example, a mobile phone or a palmtop PC with Internet access. Apparatus **100** comprises a display **102** for display of a graphical information, and a touch screen **104** for user-interaction with the apparatus. Display **102** comprises, e.g., an LCD. Touch screen **104** is, for example, a resistive tablet. For more background on such input devices, see, for example, U.S. Pat. Nos. 5,402,151; 5,231,381; 5,777,607 and 5,767,458 of Philips Electronics, all incorporated herein by reference. LCD **102** and touch screen **104** are physically integrated. Apparatus **100** comprises a random-access memory **106**, a microprocessor **108**, and a program memory **110** (e., an EEPROM). A portion of memory **106** comprises a frame buffer **112**. Frame buffer **112** is coupled to display **102** and stores the information content shown on display **102**. Memory **106** stores bitmaps that are mapped onto display **102** via frame buffer **106** under control of a software bit-blitter run on microprocessor **108**. Microprocessor **108** receives user-input via touch screen **104** and translates the input into associated GUI actions via frame buffer **112** under control of the program memory **110**. Handheld **100** comprises a wireless modem **114** for connecting to Internet **116**. Program memory **110** stores, among other things, a browser application for enabling the user to navigate the Web, and the software for processing the graphical data as explained herein.

When the user has retrieved a web page via modem **114** the page gets displayed on LCD **102** in its entirety. Due to the scale size of LCD **102** individual hyperlinks or text fragments may not be well discernible, although the lay-out of the page conveys sufficient information to the user to determine what portion of the page may be relevant. Assume that the portion is the upper right hand corner of the page. When the user now touches screen **104** in the associated location or area, this action gets translated by processor **108** and under control of program memory **110** into a zooming-in on that part of the page image that is centered around the touch location. This can be implemented, e.g., by a predetermined segmentation of the display area into, say, four areas that each can be selected for the zooming-in. Alternatively, that part of the original image gets magnified that has a center coinciding with the touch location.

User-interaction with touch screen **104** causes display **102** to undergo a change in appearance. The change is preferably effected through animation. Animation is the simulation of movement created by displaying a series of pictures, or frames, e.g., bitmaps. For example, an image of the original page gradually develops in the zoomed in version of the area selected. Through the animation, the user perceives the development from one image to the other as a continuous transition. The impression is created of a gradually changing layout. Thus, the animation avoids the impression of an abrupt confrontation with a new lay-out that requires the user to re-orientate him/herself. The animation is effected through proper processing of the bitmaps in memory **106** and frame buffer **112**.

Incorporated by reference herein are the following:

U.S. Ser. No. 09/062,364 (attorney docket PHA 23,387) filed Apr. 17, 1998 for Sung Choi and Jan van Ee for GRAPHICAL USER INTERFACE TOUCH SCREEN WITH AUTO ZOOM FEATURE. This document relates to a graphical user interface touch screen for displaying controllable functions of an electronic device. The function is displayed as an icon and at a scale size in which the function is recognizable by a user but too small to easily access features of the function. A magnified version of at least an area of the icon is provided upon the user touching the area of the icon.

In a further embodiment of the invention, the user can move across the entire keyboard by touching a particular edge of the magnified area causing magnification of the next area of the keyboard thus achieving a scrolling effect. As noted above, the keyboard embodiment is extended to any kind of graphical or displayable information. This embodiment is illustrated in FIGS. 2A-2D. In particular, FIG. 2A shows the display 102 with iconic characters "A", "B", "C", "D", "E". FIG. 2B shows the display 102 as in FIG. 2A in which a magnification window 118 is shown overlying the iconic character "A" thus enlarging this iconic character "A". In FIG. 2C, the magni-

fication window 118 is scrolled to the right such that it now overlies the iconic character "B" thus enlarging this iconic character "B", while iconic character "A" resumes its original size. Further, in FIG. 2D, the magnification window 118 is scrolled to the right such that it now overlies the iconic character "C" thus enlarging this iconic character "C", while the iconic character "B" resumes its original size.

U.S. Ser. No. 09/128,839 (attorney docket PHA 23,469) filed Aug. 4, 1998 for Jan van Ee for REMOTE CONTROL HAS ANIMATED GUI. This document relates to a remote control device for remote control of equipment such as a home theater. The remote has a display for display of a GUI that enables a user to interact with the device. User-interaction with the device causes the GUI to undergo a change in appearance. The change is effected through animation. Animation is the simulation of movement created by displaying a series of pictures, or frames, e.g., bitmaps. For example, a panel with clustered control options slides out of view and a next one slides into view, or displayed icons slide to new positions while new icons appear, etc. Through the animation, the user perceives the development from one panel to the other as a continuous transition. The impression is created of a gradually changing lay-out, of scrolling panels, of sliding, rotating, expanding or contracting icons, etc. Thus, the animation avoids the impression of an abrupt confrontation with a new lay-out.

U.S. Ser. No. 09/427,821 (attorney docket PHA 23,786) filed Oct. 27, 1999 for Joost Kemink and Richard Sagar for PDA HAS WIRELESS MODEM FOR REMOTE CONTROL VIA THE INTERNET. This document relates to a PDA combined with a wireless modem to enable remote control of CE equipment via the Internet and a local home server. More specifically, The wireless modem enables communication with a server via a data network such as the Internet. A control network is coupled between the server and controllable equipment. The handheld is now capable of functioning as a wireless remote control device for the equipment via the Internet and the server. The system may comprise a video camera together with hardware and software to create a formatted still image suitable for being displayed on the handheld device. The user can now instruct retrieval of a still image from the server via the Internet. This application serves as, e.g., a security system that enables the remote user to monitor his/her front porch, or to monitor a child by way of a remote (or fall-back) baby-sit. The user-accessibility of equipment is guaranteed by the ubiquity of the Internet, thus enabling to expand the range of control and monitoring capabilities for a mobile user.

What is claimed is:

1. A handheld communication device comprising:

a wireless modem for receiving data;

a display that has a substantially small size suitable for **[**in**]** the handheld communication device;

a data processing system connected to the modem and to the display for processing the received data and for rendering an image corresponding to the data received;

a touch screen for enabling a user to interact with the device;

wherein:

the system is operative to enable the user to select through a touch location on the touch screen a portion of the image, when displayed at a first scale, for rendering the selected portion on the display at a second scale larger than the first scale thereby facilitating a selection of a feature; and

the selected portion when rendered at the **[**first**]** *second* scale is a zoomed-in version of part of the image at the first scale substantially centered around the touch **[**screen**]** *location*.

2. The device of claim **1**, wherein a position of the touch location is arbitrary with respect to the touch screen.

3. The device of claim **1**, comprising a browser.

4. The device of claim **1**, having wireless Internet access.

5. The device of claim **1**, wherein the data comprises streaming video.

6. **[**Software for being installed on a**]** *A* handheld communication device, *comprising a non-transitory computer readable medium embodying software, the device* comprising:

a wireless modem for receiving data;

a display that has a substantially small size suitable for **[**in**]** the handheld communication device;

a data processing system connected to the input and to the display for processing the received data and for rendering an image corresponding to the data received;

a touch screen for enabling a user to interact with the device;

wherein:

the software is operative to enable the user to select through a touch location on the touch screen a portion of the image, when displayed at a first scale, for rendering the selected portion on the display at a second scale larger than the "first scale;" and, thereby facilitating a selection of a feature,

the selected portion when rendered at the **[**first**]** *second* scale is a zoomed-in version of part of the image at the first scale substantially centered around the touch **[**screen**]** *location*.

7. The handheld communication device as claimed in claim 1, wherein the data processing system is further operative to cause a window containing the selected portion displayed at the second scale to scroll across the image such that successive new selected portions of the image are displayed at the second scale.

* * * * *

11

US006211856B1

(12) United States Patent
Choi et al.

(10) Patent No.: **US 6,211,856 B1**
(45) Date of Patent: **Apr. 3, 2001**

(54) **GRAPHICAL USER INTERFACE TOUCH SCREEN WITH AN AUTO ZOOM FEATURE**

(76) Inventors: **Sung M. Choi**, 22420 Creston Dr., Los Altos, CA (US) 94024; **Jan Van Ee**, 330 Elan Village La. #130, San Jose, CA (US) 95134

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/062,364**

(22) Filed: **Apr. 17, 1998**

(51) **Int. Cl.^{7}** **G09G 5/26**; G06F 3/00; G06T 3/40

(52) **U.S. Cl.** **345/130**; 345/339; 345/439

(58) **Field of Search** 345/123, 130, 345/156, 158, 169, 173, 352, 327, 348–351, 339, 179, 168, 439; 348/734

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,746,981	*	5/1988	Nada et al.	345/127
4,751,507	*	6/1988	Hama et al.	345/131
5,001,697	*	3/1991	Torres	364/521
5,063,535	*	11/1991	Jacobs et al.	395/575
5,119,079	*	6/1992	Hube et al.	345/146
5,463,725		10/1995	Henckel et al.	395/155
5,491,495	*	2/1996	Ward et al.	345/173
5,565,888	*	10/1996	Selker	345/127
5,726,883	*	3/1998	Levine et al.	364/188
5,739,744	*	4/1998	Roca et al.	340/20
5,886,697	*	3/1999	Naughton et al.	345/348
5,956,025	*	9/1999	Goulden et al.	345/327
5,973,691	*	10/1999	Servan-Schreiber	345/342
5,986,657	*	11/1999	Berteig et al.	345/357

OTHER PUBLICATIONS

IBM, Systems Application Architecture, Jun. 1989.*

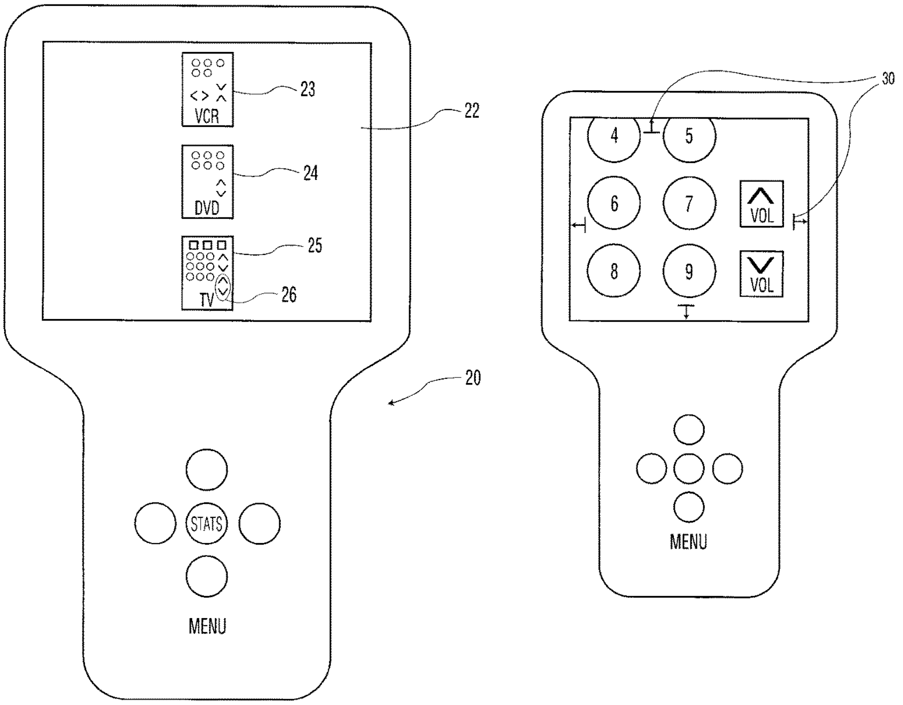
* cited by examiner

Primary Examiner—Vijay Shankar
Assistant Examiner—Manour M. Said
(74) *Attorney, Agent, or Firm*—Edward W. Goodman

(57) **ABSTRACT**

A graphical user interface "touch screen" having an entire collection of icons displayed at a scale in which the individual function of each icon is recognizable, but too small to easily access features of the function, and wherein upon touching the screen area accommodating an area of the icon, the screen provides a zoomed in version of that area so that the user can select a desired feature.

13 Claims, 3 Drawing Sheets



A-0089

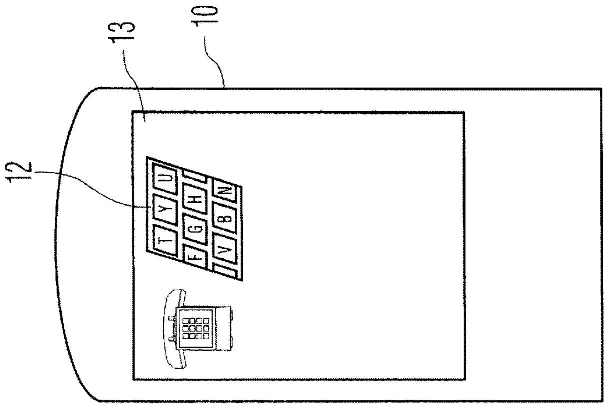


FIG. 1C

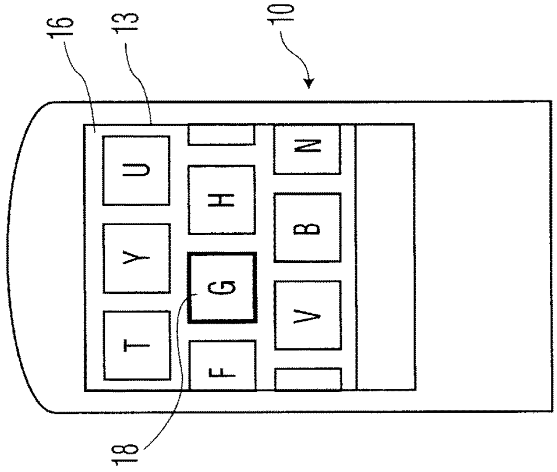


FIG. 1B

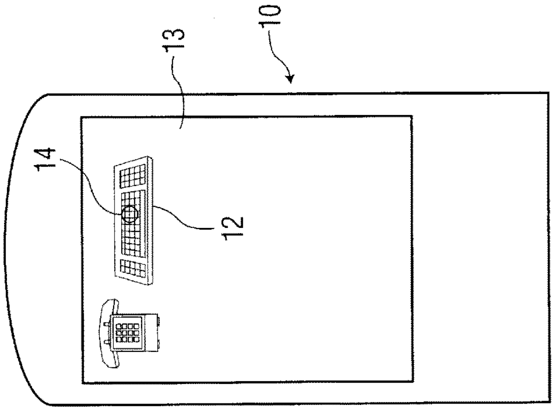


FIG. 1A

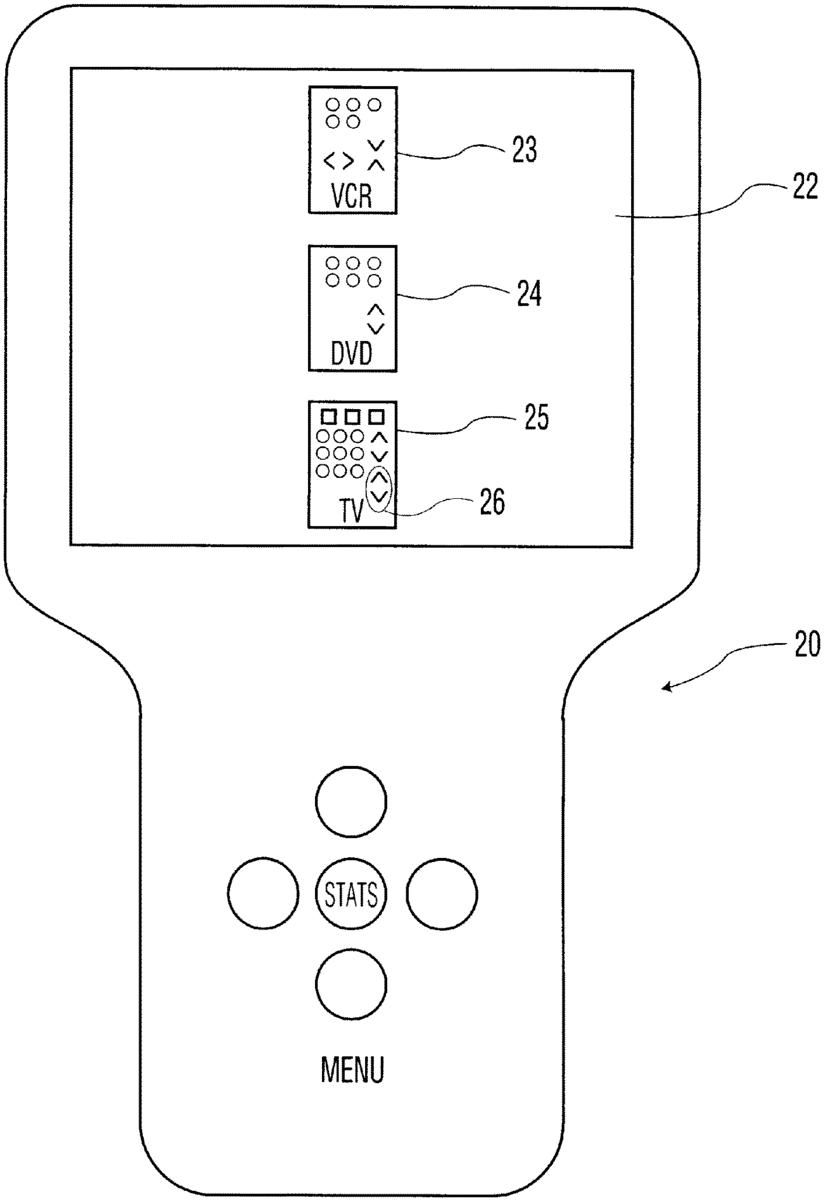


FIG. 2A

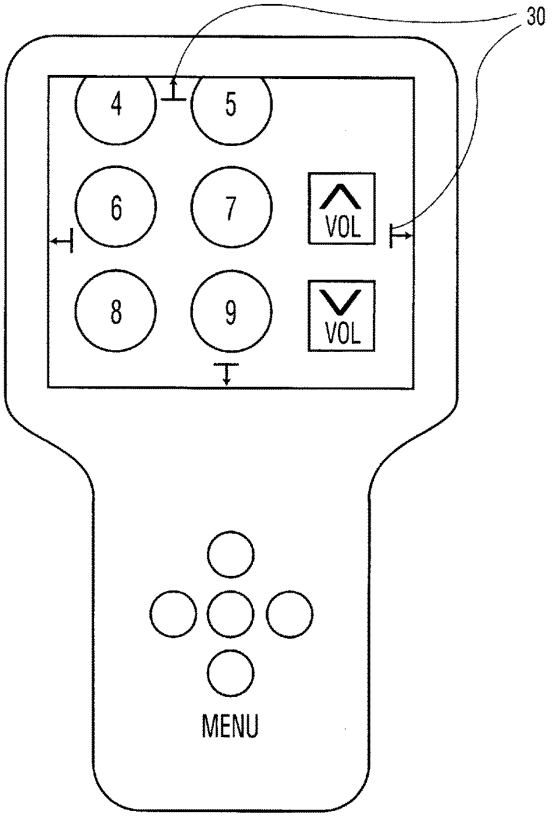


FIG. 2B

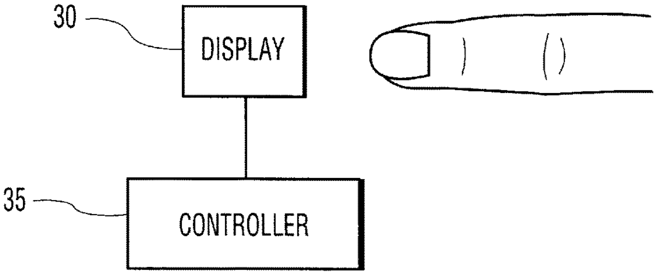


FIG. 3

GRAPHICAL USER INTERFACE TOUCH SCREEN WITH AN AUTO ZOOM FEATURE

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention relates, in general, to electronic devices having a relatively small display for providing a graphical user interface, and, in particular, to a hand-held electronic device having a graphical user interface ("GUI") and "touch screen" for accessing an entire collection of functions of the electronic device.

2. Description of the Prior Art

Icons are well known in the art of graphical user interfaces (GUI's) for controlling information processing systems. An icon is a small pictorial representation of some larger set of information. An icon provides information, in a condensed format, about the content or status of the underlying system. Icons are designed to trigger, through visual perception, operator concepts that communicate the content or operation of the system in a quick manner. The system then can be easily accessed or used through actuation of the icon.

An example of a controller unit for a home entertainment system is the Stage 3 Controller unit of Kenwood, described in Kenwood's publicly available manual "STAGE 3/ Setting up your KC-Z1 Controller", 1996. The control unit includes a hand-held controller with a touch screen functionality for the GUI. The GUI provides a large number of icons that correspond to a large number of system functionalities. The functionalities are activated through the icons on the touch screen. The GUI is user-programmable to select the icons that should be present in the main menu and those that should not. This is due to the relatively small amount of screen space available to the GUI.

Today's home entertainment systems have a large number of functions available to the user. The Kenwood Controller unit uses a GUI to extend the number of functions that are available. The problem with GUI displays for hand-held devices, such as remote controls for consumer electronic devices, for personal digital assistants (PDAs) and other portable data devices, and even for photocopiers is that they are relatively tiny. Adding the touch screen functionality to these displays means the displayed icons have to be large enough to be accessible by a person's fingers or if the icons are tiny, then they must be large enough so that some type of stylus can be used to "touch" the icon. If larger icons are used the number of functionalities to be displayed diminishes. These drawbacks limit the use of touch screen displays on hand-held devices.

SUMMARY OF THE INVENTION

Accordingly, it is an object of the invention to provide a GUI touch screen display on a hand-held device that provides a maximum number of icons on the display yet the features of the icons are easily accessible by a user.

This object is achieved by providing a zoom feature whereby a relatively small icon is provided on the GUI such that its functions are recognizable but not easily accessable by a user, but upon touch of the icon by a user the icon is made larger or magnified so that its functions can be accurately touched by a user's finger or stylus. Assuming the original icon is a picture of a keyboard, the icon in accordance with the invention is large enough to make the displayed keys "recognizable", but too small to allow individual keys to be conveniently accessed by the user. When the keyboard icon is touched by the user, in one embodiment

of the invention, the area of the icon that is touched, e.g., the keys surrounding the "G" key, is magnified or zoomed in, such that this area fills the entire space that was provided for the original keyboard icon. Alternatively in another embodiment, when the keyboard icon is touched by the user, the entire icon becomes larger to basically fill the screen of the GUI or just the area touched becomes large enough to fill the screen of the GUI.

In yet another embodiment of the invention, the user can scroll across the keyboard such that new areas become magnified.

The invention pertains to electronic devices having relatively small displays for providing touch screen GUI's and to hand-held electronic devices, such as remote controls and personal digital assistants, PDA's. The devices include a display for displaying a GUI, and a controller for enabling a user to control the system through a touch screen functionality of the GUI. The GUI provides a lay-out for each of the icons and the controller and GUI in conjunction provide a magnifying functionality that will zoom in on the icon to a magnification convenient for touch screen actuation.

The invention accordingly comprises the several steps and the relation of one or more of such steps with respect to each of the others, and the apparatus embodying features of construction, combinations of elements and arrangement of parts which are adapted to effect such steps, all as exemplified in the following detailed disclosure, and the scope of the invention will be indicated in the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is explained in further detail by way of example and with reference to the accompanying drawings, wherein:

FIG. **1***a* is a diagram of a PDA GUI touch screen showing a keyboard icon;

FIG. **1***b* is a diagram of the PDA of FIG. **1***a* after the user has touched the keyboard icon at approximately the letter "H" location;

FIG. **1***c* is a diagram of the PDA of FIG. **1***a* wherein the zoomed in area of the icon fills the icon area only;

FIG. **2***a* is a diagram of a remote control device GUI touch screen keypad showing a keyboard icon;

FIG. **2***b* is a diagram of the remote control device in FIG. **2***a* when the vol ˆ portion of the icon in FIG. **2***a* is touched; and

FIG. **3** shows the electronic device in accordance with the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Graphical user interfaces are well known in the art. U.S. Pat. No. 5,463,725, hereby incorporated by reference, is an example of a GUI with touch screen functionality.

FIGS. **1***a* and **1***b* show a PDA **10** having a touch-screen GUI **13** in accordance with the invention. The keyboard icon **12** is displayed such that it is large enough to see its functionalities, but too small for convenient touch screen activation of a single key. If a user touches area **14** of the keyboard icon **12** the resulting display **16** is shown in FIG. **1***b*. As can be seen from this display **16** the individual keys surrounding area **14** are magnified and large enough for easy touch screen activation of a single key by a finger, such as the "G" key **18** or any other nearby key. Upon releasing the "G" key **18** the key is highlighted indicating its activation and the GUI **13** then redisplays the original icon **12**. Although FIG. **1***b* shows the actual size of the icon increasing, this is not a requirement of the invention. Alternatively, the icon can stay the same size but a feature of the icon will be magnified or zoomed in on as shown in FIG. **1***c*.

In another embodiment of the invention, when the icon **12** is touched at **14** and released and the features of the icon are magnified, the user can make a selection of a key or feature and upon release of the user's finger, after key selection, the icon does not automatically return the display **16** to the initial state **12**, but instead the user can make another selection. After a predetermined time period has elapsed without a key selection being made, the icon returns to its original state **12**.

In a further embodiment of the invention, the user can move across the entire keyboard by touching a particular edge of the magnified area causing magnification of the next area of the keyboard thus achieving a scrolling effect. In this embodiment of the invention, upon selection of a function or key of the icon, the icon will return to its original size, or again the icon could remain magnified until a predetermined time period elapses without a key being selected.

FIG. **2***a* shows a remote control for a consumer electronic device **20** having a touch-screen GUI **22**. There are three icons displayed: the VCR icon **23**, the DVD icon **24** and the TV icon **25**. Each icon is too small to easily access the plurality of keys associated with the icon, however, the keys are recognizable. Upon touching one of the icons it will enlarge the area surrounding the point of touch **26** as shown in FIG. **2***b* or alternatively, if the display is large enough, all of the keys for a particular device may be accessible. The functionalities, such as scrolling **30**, explained above with regard to the PDA can also be included in the remote control. In addition the icon itself can remain the same size but a feature of the icon will be zoomed in on.

FIG. **3** shows a block diagram of the GUI touch-screen display **30** and its associated controller **35** which permits touch-screen actuation of the GUI.

It will thus be seen that the objects set forth above, among those made apparent from the preceding description, are efficiently attained and, since certain changes may be made in carrying out the above method and in the construction set forth without departing from the spirit and scope of the invention, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.

What is claimed is:

1. A graphical user interface touch screen, for displaying a user-controllable function of an electronic device, comprising:

means for displaying the function as an icon, the function corresponding to a plurality of figures, and displayed at a scale size in which the function is recognizable by a user but too small to easily select features of the plurality of features; and

means for providing a magnified version of a subset of features of the plurality of features upon the user touching an area of the icon, thereby facilitating a selection of a select one of the subset of features.

2. The graphical user interface touch screen as claimed in claim **1**, wherein the graphical user interface touch screen further comprises:

means for causing the magnified version of the subset of features to scroll across the icon such that a new subset of features of the plurality of features is magnified.

3. The graphical user interface touch screen as claimed in claim **1**, wherein the graphical user interface touch screen further comprises:

means for displaying the icon at the first scale size after selection of a feature.

4. The graphical user interface touch screen as claimed in claim **1**, wherein the graphical user interface touch screen further comprises:

means for indicating that the select one of the subset of features has been selected by the user.

5. The graphical user interface touch screen as claimed in claim **1**, wherein the a size of icon has a size is the same as a size of the magnified version of the subset of the features.

6. The graphical user interface touch screen as claimed in claim **5**, wherein the area of the icon has a corresponding location on the touch screen, and the magnified version of the subset of features is displayed at the same location on the touch screen upon the user touching the area of the icon.

7. A portable data device, comprising:

a graphical user interface touch screen that is configured to display a plurality of functions of the portable data device in the form of icons, at least one function corresponding to a plurality of features, and displayed at a scale size in which the at least one function is recognizable but too small to easily access select features of the plurality of features; and

a controller that is configured to provide a magnified version of a subset of features of the plurality of features upon a user touching an area of the icon, such that the subset of features becomes large enough for the user to easily select a feature of the subset of features and thereby control the portable data device.

8. The portable data device as claimed in claim **7**, wherein the at least one function is a keyboard function, and the plurality of features for the keyboard function corresponds to a plurality of selectable alphanumeric keys.

9. The portable data device as claimed in claim **7**, wherein the controller includes means for, upon the user touching an edge of the magnified version of the subset of features, providing a magnified version of another subset of features of the plurality of features.

10. The remote control as claimed in claim **9**, wherein the icon depicts a remote control device for a particular type of consumer electronic device, the plurality of features corresponding to individual controls of the remote control device for the particular type of consumer electronic device.

11. A remote control for controlling a consumer electronics device, comprising:

a graphical user interface touch screen which displays at least one function of the remote control in the form of an icon, the function corresponding to a plurality of features, and displayed at a scale size in which the function of an icon is recognizable but too small to easily access select a select feature of the plurality of features corresponding to the function; and

a controller that is configured to provide a magnified version of a subset of features of the plurality of features upon a user touching an area of the icon, such that the magnified version of the subset of features becomes large enough for the user to easily select one of the subset of features by touching the touch screen.

12. A method of operating an electronic device, comprising the steps:

displaying, on a graphical user interface touch screen, a function of the electronic device in the form of an icon, the function corresponding to a plurality of features, and displayed at a scale size in which the function is recognizable by a user but too small to easily select a feature of the plurality of features of the function; and

providing a magnified version of a subset of features of the plurality of features upon the user touching an area of the icon such that the magnified version becomes large enough for the user to easily access the subset of features by touching the touch screen.

13. The method of operating an electronic device as claimed in claim **11**, wherein the method further comprises the step:

scrolling the magnified version such that new subsets of the plurality of features become magnified.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,211,856 B1
APPLICATION NO. : 09/062364
DATED : April 3, 2001
INVENTOR(S) : Sung M. Choi et al.

Page 1 of 3

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 3, line 50 to Column 4, line 13 should read as follows:

1. A graphical user interface touch screen, for displaying a user-controllable function of an electronic device, comprising:
means for displaying the function as an icon, the function corresponding to a plurality of user-selectable features, the icon being displayed with the plurality of the user-selectable features, and the icon being displayed at a first scale size; and
means for displaying a subset of the displayed features at a second scale size that is larger than the first scale size, upon a user touching an area of the icon, thereby facilitating a selection of a select one of the subset of features.

2. The graphical user interface touch screen as claimed in claim 1, wherein the graphical user interface touch screen further comprises:
means for causing the subset of the features displayed at the second scale size to scroll across the icon such that a new subset of the features is displayed at the second scale size.

3. The graphical user interface touch screen as claimed in claim 1, wherein the graphical user interface touch screen further comprises:
means for displaying the icon at the first scale size after selection of a feature.

4. The graphical user interface touch screen as claimed in claim 1, wherein the graphical user interface touch screen further comprises:
means for indicating that the select one of the subset of features has been selected by the user.

5. The graphical user interface touch screen as claimed in claim 1, wherein a size of the icon is substantially the same as a further size of the subset of the features displayed at the second scale size.

Signed and Sealed this
Seventh Day of August, 2012

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office

Column 4, line 14 to Column 4, line 47 should read as follows:

6. The graphical user interface touch screen as claimed in claim 5, wherein the area of the icon has a corresponding location on the touch screen, and the subset of the features displayed at the second scale size is displayed in substantially the same location on the touch screen upon the user touching the area of the icon.

7. A portable data device, comprising:
a graphical user interface touch screen that is configured to display a user-controllable function as an icon, the function corresponding to a plurality of user-selectable features, the icon being displayed with the plurality of the user-selectable features, and the icon being displayed at a first scale size; and
a controller to control displaying a subset of the displayed features at a second scale size that is larger than the first scale size, upon a user touching an area of the icon.

8. The portable data device as claimed in claim 7, wherein the function comprises a keyboard function, and the plurality of features for the keyboard function corresponds to a plurality of selectable alphanumeric keys.

9. The portable data device as claimed in claim 7, wherein the controller includes means for, upon the user touching an edge of the subset of the features displayed at the second scale size, causing another subset of the features to be displayed at the second scale size.

10. The remote control as claimed in claim 11, wherein the icon depicts a remote control device for a particular type of consumer electronic device, the plurality of features corresponding to individual controls of the remote control device for the particular type of consumer electronic device.

Column 4, line 48 to Column 6, line 5 should read as follows:

11. A remote control for controlling a consumer electronics device, comprising:
a graphical user interface touch screen which displays a user-controllable function of the remote control as an icon, the function corresponding to a plurality of user-selectable features, the icon being displayed with the plurality of the user-selectable features, and the icon being displayed at a first scale size; and
a controller to control displaying a subset of the features at a second scale size that is larger than the first scale size, upon a user touching an area of the icon.

12. A method of operating an electronic device, comprising the steps:
displaying, on a graphical user interface touch screen, a function of the electronic device as an icon, the function corresponding to a plurality of user-selectable features, the icon being displayed with the plurality of the user-selectable features, and the icon being displayed at a first scale size; and
displaying a subset of the features at a second scale size that is larger than the first scale size, upon the user touching an area of the icon.

13. The method of operating an electronic device as claimed in claim 12, wherein the method further comprises the step:

scrolling the subset of features displayed at the second scale size such that new subsets of the plurality of features become displayed at the second scale size.

12

UNITED STATES PATENT AND TRADEMARK OFFICE

51

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/156,409	05/28/2002	Matthew J. Bickerton	GB 010099	5236

24737 7590 10/06/2004

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
EDWARDS JR, TIMOTHY	
ART UNIT	**PAPER NUMBER**
2635	

DATE MAILED: 10/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Notice of Allowability	**Application No.** 10/156,409	**Applicant(s)** BICKERTON, MATTHEW J.	
	Examiner Timothy Edwards, Jr.	**Art Unit** 2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *filing date May 28, 2002*.

2. ☒ The allowed claim(s) is/are *1-6 and 8*.

3. ☒ The drawings filed on *28 May 2002* are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☒ All b) ☐ Some* c) ☐ None of the:

   1. ☒ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Greg Thorne on September 27, 2004.

The application has been amended as follows:

IN THE CLAIMS:

Please cancel claim 7.

Allowable Subject Matter

Claims 1-6,8 are allowed.

The following is an examiner's statement of reasons for allowance: in the environment of a keypad for inputting a character to a device, the closes prior art Curtin et al '980, who discloses a computer data entry method having means to display each of a plurality of characters after selecting a first key. However, Curtin fails to teach or suggest, a keypad in a default state displaying the primary character associated with a key in its respective display area, displaying a selected primary key's secondary characters in a respective display area, selecting a second key which is associated with the secondary character desired for input, and returning the keypad to the default state.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is Nowlan et al '538, Yu et al '006, Chang et al '142, Balakrishnan et al '942, Vale '572, Curtin et al '980, Grover et al '437 and Knowlton et al '273. Disclosed prior art addresses the use of an input device, having numerous characters per key, for interpreting ambiguous input.

2. Any inquiry concerning this communication should be directed to Examiner Timothy Edwards at telephone number (571) 272-3067. The examiner can normally be reached on Monday-Thursday, 8:30 a.m.-4:00 p.m. The examiner cannot be reached on Fridays.

If attempt to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik, can be reached on (571) 272-3068.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-4700, Mon-Fri., 8:30 a.m.-5:00 p.m.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

or fax to:

(703), 872-9314 (for formal communications intended for entry)

Or:

(for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Sixth Floor, (Receptionist).

Timothy Edwards, Jr.
Primary Examiner
September 27, 2004

13

2154

#8/A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	**Yevgeniy Eugene Shteyn**	Attorney Docket No.:	**PHA 23.782**
Appl. No.:	**09/433,257** Conf.: **2314**	Art Unit:	**2154**
Filed:	**11/4/1999**	Examiner:	**Lin, Wen Tai**

3/27/03

Title: **Partitioning of MP3 Content File for Emulating Streaming**

Box Non-Fee Amendment
Assistant Commissioner for Patents
Washington, D.C. 20231

AMENDMENT TRANSMITTAL

Sir:

Enclosed is an Amendment under 37 CFR 1.111, in the above-identified application. A total of 29 pages, including this transmittal, are being submitted at this time.

The Commissioner is hereby requested and authorized pursuant to 37 CFR §1.136(a)(3), to treat any concurrent or future reply in this application requiring a petition for extension of time for its timely submission, as incorporating a petition for extension of time for the appropriate length of time. Please charge any additional fees which may now or in the future be required in this application, including extension of time fees, but excluding the issue fee unless explicitly requested to do so, and credit any overpayment, to Deposit Account No. 14-1270.

Date: 10/3/02

Respectfully submitted,

By
Michael J. Ure
Attorney, Reg No. ~~45,110~~ 33,089
(408) 617-4742

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first-class mail in an envelope addressed to: Assistant Commissioner for Patents
Washington, D.C. 20231

By Shannon Lester on 10/3/2002

A-0104

14. A method of, at a client device, forming a media presentation from multiple related files, including a control information file, stored on one or more server computers within a computer network, the method comprising:

downloading the control information file to the client device;

the client device parsing the control information file; and

based on parsing of the control information file, the client device:

retrieving a first file and using contents of the first file to begin a media presentation;

concurrent with the media presentation, retrieving a next file; and

using content of the next file to continue the media presentation.

15. The method of claim 14 wherein the control information file is an XML file.

16. The method of claim 15, wherein the XML file identifies multiple alternative files corresponding to a given segment of the media presentation, further comprising selecting and retrieving one of the multiple alternative files.

17. A method of storing media presentation information within a computer network including multiple server computers, the method comprising:

storing on a server computer a control information file of a format to be parsed by a client device; and storing on one or more server computers multiple related files accessible by the client device to, based on parsing of the control information file, form a media presentation from the multiple related files.

18. The method of claim 17, wherein the control information file is an XML file.

19. The method of claim 18, wherein the XML file identifies multiple alternative files corresponding to a given segment of the media presentation.

20. A client device for forming a media presentation from multiple related files stored on server computers within a computer network, comprising:

means for downloading files to the client device;

means for parsing a control information file; and

means for, based on parsing of the control information file:

retrieving a first file and using contents of the first file to begin a media presentation;

concurrent with the media presentation, retrieving a next file; and

using content of the next file to continue the media presentation.

21. The method of claim 20, wherein the control information file is an XML file.

22. The method of claim 21, wherein the XML file identifies multiple alternative files corresponding to a given segment of the media presentation, the means for retrieving comprising means for selecting and retrieving one of the multiple alternative files.

Please amend claims 2-6, 12 and 13 as follows:

2. The method of claim ~~1~~ 14, wherein ~~the~~ partitioning of media presentation information between the multiple related files is determined by information about the client.

3. The method of claim ~~1~~ 14, wherein ~~the~~ partitioning of media presentation information between the multiple related files is determined by information about the computer network.

4. The method of claim ~~1~~ 14, wherein the ~~file~~ media presentation comprises an audio presentation ~~file~~.

5. The method of claim ~~1~~ 14, wherein the ~~file~~ media presentation comprises a video presentation ~~file~~.

6. The method of claim ~~1~~ 14, wherein ~~the~~ partitioning of media presentation information between the multiple related files ~~comprises adding respective~~ is described within the control information file using tags corresponding to respective ~~ones of the segments~~ files.

12. The device of claim ~~11~~ 18, wherein:
~~- the content information is accessible through control information provided to the device; and~~
- the device ~~is capable of interpreting~~ interprets the control information to retrieve ~~the segments~~ multiple files from the ~~server~~ computer network for sequential play-out.

I CLAIM:

2. The method of claim 14, wherein partitioning of media presentation information between the multiple related files is determined by information about the client.

3. The method of claim 14, wherein partitioning of media presentation information between the multiple related files is determined by information about the computer network.

4. The method of claim 14, wherein the media presentation comprises an audio presentation.

5. The method of claim 14, wherein the media presentation comprises a video presentation.

6. The method of claim 14, wherein partitioning of media presentation information between the multiple related files is described within the control information file using tags corresponding to respective files.

12. The device of claim 18, wherein:
- the device interprets the control information to retrieve multiple files from the computer network for sequential play-out.

13. The device of claim 12, wherein:
- the means for parsing comprises an XML parser; and
- the means for retrieving and using comprises an XML interpreter.

14. A method of, at a client device, forming a media presentation from multiple related files, including a control information file, stored on one or more server computers within a computer network, the method comprising:

downloading the control information file to the client device;

the client device parsing the control information file; and

based on parsing of the control information file, the client device:

retrieving a first file and using contents of the first file to begin a media presentation;

concurrent with the media presentation, retrieving a next file; and

using content of the next file to continue the media presentation.

15. The method of claim 14 wherein the control information file is an XML file.

16. The method of claim 15, wherein the XML file identifies multiple alternative files corresponding to a given segment of the media presentation, further comprising selecting and retrieving one of the multiple alternative files.

17. A method of storing media presentation information within a computer network including multiple server computers, the method comprising:

storing on a server computer a control information file of a format to be parsed by a client device; and

storing on one or more server computers multiple related files accessible by the client device to, based on parsing of the control information file, form a media presentation from the multiple related files.

18. The method of claim 17, wherein the control information file is an XML file.

19. The method of claim 18, wherein the XML file identifies multiple alternative files corresponding to a given segment of the media presentation.

20. A client device for forming a media presentation from multiple related files stored on server computers within a computer network, comprising:

means for downloading files to the client device;

means for parsing a control information file; and

means for, based on parsing of the control information file:

retrieving a first file and using contents of the first file to begin a media presentation;

concurrent with the media presentation, retrieving a next file; and

using content of the next file to continue the media presentation.

21. The method of claim 20, wherein the control information file is an XML file.

22. The method of claim 21, wherein the XML file identifies multiple alternative files corresponding to a given segment of the media presentation, the means for retrieving comprising means for selecting and retrieving one of the multiple alternative files.

13. The device of claim 12, wherein:
~~- the control information comprises an XML format;~~
- the ~~device has~~ means for parsing comprises an XML parser; and
- the ~~device has~~ means for retrieving and using comprises an XML interpreter.

A clean copy of the amended claims is included as part of the substitute specification.

REMARKS

The Office Action of 08/20/2002 has been carefully considered. In response thereto, the specification and claims have been amended for greater clarity. A substitute specification is submitted herewith. Reconsideration is respectfully requested.

Claims 1-13 were objected to for various informalities. These informalities have been corrected by the present amendments.

Claims 7-10 were rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Claim 7 has been cancelled in favor of new claim 17, which is believed to present statutory subject matter.

Claims 1-5 and 12 were rejected as being anticipated by or unpatentable over Gelman. Claim 6-9 were rejected as being unpatentable over Gelman in vie wof Cohen. Finally, claims 10 and 13 were rejected as being unpatentable over Gelman in view of Girardot. Claims 1 and 12 have been cancelled in favor of new independent claims 14 and 20. Reconsideration is respectfully requested.

The present invention relates to a flexible, client-driven method of media retrieval and presentation, as well as an intelligent client device for carrying out such method. In an exemplary embodiment, the method uses a parseable control information file such as an XML file. Media retrieval and presentation begins with retrieval and parsing of the control information file. A control script is then run by an XML interpreter, using output from the XML parser. In general, the control script retrieves files, or segments of the media presentation, from one or more servers in a computer network for sequential play-out. Insofar as the particulars of which files are retrieved, when and from where, however, the control script offers great flexibility. For example, two or more alternative files may be provided corresponding to the same section of a media presentation, with the client device selection between the alternatives based on device capability, for example, or network conditions, or other considerations.

Gindele does not teach or suggest such a modified prefetch strategy. Gindele does describe prefetch and a LRU (least recently used) replacement algorithm. A similar LRU algorithm as applied in Gindele to *cache lines* is applied in a subsidiary aspect of the invention to *cache buffer registers* (as opposed to cache lines themselves).

Nevertheless, the prefetch strategy of Gindele is clearly different from that of the present invention. As described in the second paragraph, lines 4-9, a prefetch is initiated by the first CPU reference to a block after it is put into the cache, the prefetch transferring to the cache the next sequential block after the block having the cache hit. No consideration is made, as in the present invention, of *where* in the cache line (or block) the hit occurred. Accordingly, independent claims 12 and 13 are believed to patentably define over the cited reference.

Dependent claims 2-5, 15, 16, 18, 19, 21 and 22 are also believed to add novel and patentable subject matter to their respective independent claims. Withdrawal of the rejection and allowance of claims 2-6 and 12-22 is respectfully requested.

Respectfully submitted,

Michael J. Ure, Reg. 33,089

Dated: October 1, 2002

14

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE WITH SUFFICIENT POSTAGE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: MAILSTOP APPEAL BRIEF, ASSISTANT COMMISSIONER OF PATENTS AND TRADEMARKS, P.O. BOX 1450, ALEXANDRIA, VA, 22313-1450, ON:

#12

Date:__________________ By:________________________

PATENT
Attorney's Docket No. PHA 23.782

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

SHTEYN

Application No.: 09/433,257

Filed: 11/04/1999

For: PARTITIONING OF MP3 CONTENT FILE FOR EMULATING STREAMING

Group Art Unit: 2154

Examiner: Wen Tai Lin

Appeal No.__________

BRIEF FOR APPELLANT

Mailstop APPEAL BRIEF
Assistant Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This appeal is from the decision of the Primary Examiner dated 04/07/2003, finally rejecting claims 2-6 and 12-22, which are reproduced as an Appendix to this brief.

The Commissioner is authorized to charge the fee of $320, and any other fees that may be required by this paper, to Deposit Account No. 14-1270.

(1) Real Party in Interest

The real party in interest is the assignee, Philips Electronics North America Corporation.

(2) Related Appeals or Interferences

Applicant is not aware of any related appeals or interferences.

(3) Status of Claims

Claims 2-6 and 12-22 remain pending in the present application. All claims have been finally rejected and all claims are on appeal.

(4) Status of Amendments

All amendments have been entered. No amendment after final has been submitted.

(5) Summary of the Invention

The present invention relates to a flexible, client-driven method of media retrieval and presentation, as well as an intelligent client device for carrying out such method. In an exemplary embodiment, the method uses a parseable control information file such as an XML file. Media retrieval and presentation begins with retrieval and parsing of the control information file. A control script is then run by an XML interpreter, using output from the XML parser. In general, the control script retrieves files, or segments of the media presentation, from one or more server s in a computer network for sequential playout. Insofar as the particulars of which files are retrieved, when and from where, however, the control script offers great flexibility. For example, two or more alternative files may be provided corresponding to the same section of a media presentation, with the client device selecting between the alternatives based on device capability, for example, or network conditions, or other considerations.

(6) The References

The rejections are based on Cohen, U.S. Patent 5,751,968. Those claims not rejected based solely on Cohen have been rejected based on Cohen in view of Giradot, "Efficient Representation and Streaming of XML Content Over the Internet Medium."

Cohen teaches a client/server content streaming system. On the server side, the server forms from a multi-media presentation segment data files. On the client side, an interactive display application (i.e., player software) receives the files from the server and displays the multi-media presentation.

Giradot describes a system for efficient encoding and streaming of XML content. Giradot, however, is not prior art with respect to the present application.

(7) The Rejections

In the Final Rejection of April 7, 2003, claims 4-6, 14, 17 and 20 were rejected under 35 USC 102(b) as being anticipated by Cohen. The rejection states in part:

> Cohen taught the invention as claimed including ... the client device parsing the control information file [58, Fig. 5; note that parsing is an inherent function of a browser]....

Claims 2 and 3 were rejected as being unpatentable over the Cohen. With respect to these claims, the Office Action admits that Cohen does not teach or suggest the features of these claims but takes official notice that the recited features are well-known.

Claims 12, 13, 15, 16, 18, 19, 21 and 22 were rejected as being unpatentable over Cohen in view of Giradot.

(8) Issues

The following issues are presented:

1. Whether claims 4-6, 14, 17 and 20 are anticipated by Cohen.

2. Whether claims 2 and 3 would have been obvious in view of Cohen.

3. Whether claims 12, 13, 15, 16, 18, 19, 21 and 22 would have been obvious from Cohen in view of Giradot.

(9) Argument

Addressing now the rejection under 35 USC 102 based on Cohen, the rejection states in part:

> Cohen taught the invention as claimed including … the client device parsing the control information file [58, Fig. 5; note that parsing is an inherent function of a browser]….

Applicant respectfully disagrees. As described in column 6 of Cohen, clicking a link associated with the "connection file" of a desired media presentation causes an interactive display application—i.e., a proprietary media player--to be activated. The media player knows *a priori* the format of the connection file, which therefore need not be parsed. The connection file and the media player must be updated, if at all, in lock-step. The resulting system is rigid and inflexible.

The connection file in Cohen is *not* received and acted upon by the browser, which Applicant agrees does perform parsing in order to render content. Rather, it is received and acted upon by the interactive display application, or media player.

Accordingly, claims 4-6, 14, 17 and 20 are not believed to be anticipated by Cohen.

Addressing now the obviousness rejection of claims 2 and 3, the Office Action admits that Cohen does not teach or suggest the features of these claims but takes official notice that the recited features are well-known. Applicant disagrees and respectfully requests that prior art addressing this point be cited. Nevertheless, claims 2 and 3 are believed to patentable at least for the same reasons as independent claim 14.

Finally, with respect to the rejection based on Cohen in view of Giradot, there is no indication in the record that Giradot was published earlier than the year 2000. The present application was filed 11/04/1999. Accordingly, Giradot is not prior art with respect to the present application.

(10) CONCLUSION

For the foregoing reasons, claims 4-6, 14, 17 and 20 are not anticipated by Cohen, nor would claims 2 and 3 have been obvious in view of the same. Claims 12, 13, 15, 16, 18, 19, 21 and 22 would not have been obvious from Cohen in view of Giradot.

Applicant respectfully submits therefore that the Final Rejection should be REVERSED.

Respectfully submitted,

By:____________________
Michael J. Ure
Attorney for Applicant
Registration No. 33,089

Date: September 8, 2003

15

#15
Turner B
2/24/04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of YEVGENIY EUGENE SHTEYN	Atty. Docket PHA-28.782
Serial: 09/433,257	Group Art Unit: 2314
Filed: 11/04/1999	Examiner: LIN, WEN TAI

PARTITIONING OF MP3 CONTENT FILE FOR EMULATING STREAMING

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE UNDER 37 C.F.R. 1.111

Sir:

The following Remarks are responsive to the Office Action of October 20, 2003.

REMARKS

The Office Action of October 20, 2003 has been carefully considered. Reconsideration in view of the following remarks is respectfully requested.

The present invention relates to a flexible, client-driven method of media retrieval and presentation, as well as an intelligent client device for carrying out such method. In an exemplary embodiment, the method uses a parseable control information file such as an XML file. Media retrieval and presentation begins with retrieval and parsing of the control information file. A control script is then run by an XML interpreter, using output from the XML parser. In general, the control script retrieves files, or segments of the media presentation, from one or more server s in a computer network for sequential playout. Insofar as the particulars of which files are retrieved, when and from where, however, the control script offers great flexibility. For example, two or more alternative files may be provided corresponding to the same section of a media presentation, with the client device selecting between the alternatives based on device capability, for example, or network conditions, or other considerations.

Claims 4-6, 14, 17 and 20 were rejected under 35 USC 102(b) as being anticipated by Cohen. Claims 2 and 3 were rejected as being unpatentable over the same reference further in view of Lin et al. ("Lin"). Claims 12, 13, 15, 16, 18, 19, 21 and 22 were rejected as being unpatentable over Cohen in view of Bayeh et al. ("Bayeh"). The rejections are respectfully traversed.

Addressing now the rejection under 35 USC 102 based on Cohen, the rejection states in part:

> Cohen taught the invention as claimed including … the client device parsing the control information file [58, Fig. 5; note that parsing is an inherent function of a browser]….

Applicant respectfully disagrees. As described in column 6 of Cohen, clicking a link associated with the "connection file" of a desired media presentation causes an interactive display application—i.e., a proprietary media player--to be activated. The media player know *a priori* the format of the connection file, which therefore need not be parsed. The connection file and the media player must be updated, if at all, in lock-step. The resulting system is rigid and inflexible.

The connection file in Cohen is *not* received and acted upon by the browser, which Applicant agrees does perform parsing in order to render content. Rather, it is received and acted upon by the interactive display application, or media player.

Accordingly, claims 4-6, 14, 17 and 20 are not believed to be anticipated by Cohen.

With respect to claims 2 and 3, the combination of Lin with Cohen does not remedy the deficiencies of Cohen. Claims 2 and 3 are therefore believed to be patentable at least for the same reasons as claim 14.

With respect to claims 12, 13, 15, 16, 18, 19, 21 and 22, the combination of Bayeh with Cohen still fails to teach or suggest the salient features of these claims.

Bayeh teaches the separation of underlying data and format information to be applied to that data in storing and serving up web-based information. Referring to the cover figure of Bayeh, the data may be stored in the form of XML, while the format may be stored in the form of XSL ("Extensible Style Language"). When a web page is requested, the XML data is retrieved so that the XSL format information may be applied to it to form a *conventional* HTML data stream 96'. Such a conventional HTML data stream is what is received by the client computer. That is, from the standpoint of the client, it neither knows or cares whether the arrangement of Bayeh is used, as it makes no difference to the operation of the client.

The Office Action states in part: "[I]t would have been obvious…that Cohen's connection file could have been written as an XML file, because XML is more flexible in defining control/information tags." However, as may be appreciated from the foregoing discussion, taking Cohen and Bayeh in combination, it would not have been obvious for the client to receive a connection file written as XML. There is no teaching whatsoever within the four corners of the references themselves to support this contention.

For the foregoing reasons, claims 14, 17 and 20 are believed to patentably define over Cohen. Dependent claims 2-6, 12, 13, 15, 1618, 19, 21 and 22 are also believed to add novel and patentable subject matter to their respective independent claims. Withdrawal of the rejection and allowance is respectfully requested.

Respectfully submitted,

Michael J. Ure, Reg. 33,089

Dated: February 19, 20042

16

I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE WITH SUFFICIENT POSTAGE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: MAILSTOP APPEAL BRIEF, ASSISTANT COMMISSIONER OF PATENTS AND TRADEMARKS, P.O. BOX 1450, ALEXANDRIA, VA, 22313-1450, ON:

Date: 7/28/2004 By: DANIEL MICHALEK

PATENT
Attorney's Docket No. PHA 23.782

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

SHTEYN

Application No.: 09/433,257

Filed: 11/04/1999

For: PARTITIONING OF MP3 CONTENT FILE FOR EMULATING STREAMING

Group Art Unit: 2154

Examiner: Wen Tai Lin

Appeal No.__________

BRIEF FOR APPELLANT

Mailstop APPEAL BRIEF
Assistant Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This appeal is from the decision of the Primary Examiner dated 03/25/2004, finally rejecting claims 2-6, 14, 17 and 20, which are reproduced as an Appendix to this brief.

The Commissioner is authorized to charge the fee of $330, and any other fees that may be required by this paper, to Deposit Account No. 14-1270.

(1) Real Party in Interest

The real party in interest is the assignee, Philips Electronics North America Corporation.

(2) Related Appeals or Interferences

Applicant is not aware of any related appeals or interferences.

(3) Status of Claims

Claims 2-6 and 12-22 remain pending in the present application. Claims 2-6, 14, 17 and 20 have been finally rejected and are on appeal.

(4) Status of Amendments

All amendments have been entered. No amendment after final has been submitted.

(5) Summary of the Invention

The present invention relates to a flexible, client-driven method of media retrieval and presentation, as well as an intelligent client device for carrying out such method. In an exemplary embodiment, the method uses a parseable control information file such as an XML file. Media retrieval and presentation begins with retrieval and parsing of the control information file. A control script is then run by an XML interpreter, using output from the XML parser. In general, the control script retrieves files, or segments of the media presentation, from one or more server s in a computer network for sequential playout. Insofar as the particulars of which files are retrieved, when and from where, however, the control script offers great flexibility. For example, two or more alternative files may be provided corresponding to the same section of a media presentation, with the client device selecting between the alternatives based on device capability, for example, or network conditions, or other considerations.

(6) The References

The rejections are based on Cohen, U.S. Patent 5,751,968. Those claims (claim 2 and 3) not rejected based solely on Cohen have been rejected based on Cohen in view of Lin, U.S. Patent 6,405,256.

Cohen teaches a client/server content streaming system. On the server side, the server forms from a multi-media presentation segment data files. On the client side, an interactive display application (i.e., player software) receives the files from the server and displays the multi-media presentation.

Lin describes a data streaming transmission method and system in which a network server communicates with a client device through a network. Within the network, communications pass through some number of caching servers, each having an expandable buffer. As illustrated in Figure 2 thereof, data segments are in effect queued up within a series of cache servers, with data segments occurring earlier in order being queued up within cache servers nearer the client device. Upstream caching servers send data segments at a constant rate to their next downstream caching servers. If there is network congestion between an upstream caching server and a downstream caching server, steps are taken to absorb that congestion, if possible without adversely impacting overall streaming, e.g., by decreasing the streaming rate from the upstream caching server and/or increasing the buffer size in the downstream caching server. When the buffer approaches overflow, streaming is temporarily discontinued. When congestion subsides, streaming resumes, and the streaming rate and the buffer size are opportunitstically increased and decreased, respectively.

(7) The Rejections

In the Final Rejection of March 25, 2004, claims 4-6, 14, 17 and 20 were rejected under 35 USC 102(b) as being anticipated by Cohen. The rejection states in part:

> Cohen taught the invention as claimed including … the client device parsing the control information file [58, Fig. 5; col. 6, lines 26-50; i.e., the interactive display application program must parse the connection file in order to obtain the reference for segment file and its associated status]….

Claims 2 and 3 were rejected as being unpatentable over Cohen in view of Lin. The rejection states in part:

> [I]t would have been obvious … that Cohen's data file size should be a factor of the client's buffering and display capability because this criterion makes sure that the data streaming in Cohen's media presentation can be achieved without overflowing the client's buffering capacity [col. 5, lines 39-53].

(8) Issues

The following issues are presented:

1. Whether claims 4-6, 14, 17 and 20 are anticipated by Cohen.

2. Whether claims 2 and 3 would have been obvious from Cohen in view of Lin.

(9) Argument

Addressing now the rejection under 35 USC 102 based on Cohen, the rejection states in part:

> Cohen taught the invention as claimed including ... the client device parsing the control information file [58, Fig. 5; col. 6, lines 26-50; i.e., the interactive display application program must parse the connection file in order to obtain the reference for segment file and its associated status]....

Applicant respectfully disagrees. As described in column 6 of Cohen, clicking a link associated with the "connection file" of a desired media presentation causes an interactive display application—i.e., a proprietary media player--to be activated. The media player knows *a priori* the format of the connection file, which therefore need not be parsed. The connection file and the media player must be updated, if at all, in lock-step. The resulting system is rigid and inflexible.

The connection file in Cohen is *not* received and acted upon by the browser, which Applicant agrees does perform parsing in order to render content. Rather, it is received and acted upon by the interactive display application, or media player.

Accordingly, claims 4-6, 14, 17 and 20 are not believed to be anticipated by Cohen.

Claims 2 and 3 are believed to patentable at least for the same reasons as independent claim 14.

(10) CONCLUSION

For the foregoing reasons, claims 4-6, 14, 17 and 20 are not anticipated by Cohen, nor would claims 2 and 3 have been obvious in view of the same.

Applicant respectfully submits therefore that the Final Rejection should be REVERSED.

Respectfully submitted,

By:
Michael J. Ure
Attorney for Applicant
Registration No. 33,089

Date: July 27, 2004

17

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/433,257	11/04/1999	YEVGENIY EUGENE SHTEYN	PHA-23.782	2314

24738 7590 10/05/2004

PHILIPS ELECTRONICS NORTH AMERICA CORPORATION
INTELLECTUAL PROPERTY & STANDARDS
1109 MCKAY DRIVE, M/S-41SJ
SAN JOSE, CA 95131

EXAMINER	
LIN, WEN TAI	
ART UNIT	**PAPER NUMBER**
2154	

DATE MAILED: 10/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	**Application No.** 09/433,257	**Applicant(s)** SHTEYN, YEVGENIY EUGENE	
	Examiner Wen-Tai Lin	**Art Unit** 2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-6 and 12-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-6 and 12-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 2-6 and 12-22 are presented for examination.

2. The prosecution of this instant application is re-opened because a new prior art, McLain [U.S. Pat. No. 6493758], is found. The finality of the previous office action is hereby withdrawn in view of the new ground of rejection set forth below.

3. The text of those sections of Title 35, USC code not included in this action can be found in the prior Office Action.

Claim Rejections - 35 USC § 103

4. Claims 4-6 and 12-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen [U.S. Pat. No. 5751968] in view of McLain [U.S. Pat. No. 6493758].

5. Cohen was cited in the previous office action.

6. As to claims 14-15, Cohen teaches the invention substantially as claimed including: a method of, at a client device, forming a media presentation from multiple related files, including a control information file [54, Fig.5; col.6, lines 26-40], stored on one or more server computers within a computer network, the method comprising:

downloading the control information file to the client device [56, Fig.5];

the client device parsing the control information file [58, Fig.5; col.6, lines 26-40; i.e., the interactive display application program must parse the connection file in order to obtain the reference for segment file and its associated status]; and

based on the control information file, the client device:

retrieving a first file and using contents of the first file to begin a media presentation [60, Fig.5; col.6, lines 41-44];

concurrent with the media presentation, retrieving a next file; and

using content of the next file to continue the media presentation [64, Fig.5; col.6, lines 44-54].

Cohen does not specifically teach how the connection file is formed and using what format. That is, Cohen does not indicate whether the parameters contained in the control information file are extracted via parsing or not. However, in the same field of endeavor, McLain teaches that the control information file may be written in the form of XML file and use the browser's parser for extracting parameters therein [McLain: see col.1, lines 43-65].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have used XML as an alternative format for composing Cohen's connection file because XML is well known for its flexibility, with which it would make Cohen's connection file more dynamic and adaptable for containing the rather sophisticated file status information [col.6, lines 26-40].

7. As to claims 4-5, Cohen further teaches that the media presentation comprises an audio presentation or a video presentation [col.1, lines 49-54].

8. As to claim 6, Cohen in view of McLain teaches that partitioning of media presentation information between the multiple related files is described within the control information file using tags corresponding to respective files [i.e., XML uses tags for specifying various parameters and values].

9. As to claim 16, Cohen in view of McLain further teaches that the XML file identifies multiple alternative files corresponding to a given segment of the media presentation, the method further comprising selecting and retrieving one of the multiple alternative files [Cohen: col.6, line 63 – col.7, line 5].

10. As to claims 12-13 and 17-22, since the features of these claims can also be found in claims 4-6 and 14-16, they are rejected for the same reasons set forth in the rejection of claims 4-6 and 14-16 above.

11. Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen [U.S. Pat. No. 5751968], as applied to claims 4-6 and 12-22 above and McLain [U.S. Pat. No. 6493758], as applied to claims 4-6 and 12-22 above, further in view of Lin et al.(hereafter "Lin")[U.S. Pat. No. 6405256].

12. Lin was cited from the previous office action.

13. As to claim 2, Cohen does not specifically teach that partitioning of media presentation information between the multiple related files is determined by information about the client.

However, Lin teaches a data streaming method/system wherein partitioning of streamed data is based on the buffering capability of the client device [Lin: col.6, lines 47-50]. It would have been obvious to one of ordinary skill in the art at the time the invention was made that Cohen's data file size should be a factor of the client's buffering and display capability because this criterion makes sure that data streaming in Cohen's media presentation can be achieved without overflowing the client's buffering capacity [col.5, lines 39-53].

14. As to claim 3, Cohen does not specifically teach that partitioning of media presentation information between the multiple related files is determined by information about the computer network.

However, Lin teaches a network comprising a plurality of caching servers, each with expandable buffer for storing additional segments of streamed data for absorbing network congestion [Abstract]. Since the caching servers and the network congestion are part of the information of the network, it is obvious that the data segmentation in Cohen's network, which obviously also comprises a plurality of communication nodes, should also be based on the network's buffering capability in each intermediate network node, because by doing so one would be able to anticipate Cohen system's tolerance against traffic fluctuation.

15. Claims 2-6 and 12-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over McLain [U.S. Pat. No. 6493758] in view of White et al. (hereafter "White") [U.S. Pat. No. 6005563].

16. As to claims 14-15, McLain teaches the invention substantially as claimed including: a method of, at a client device, forming a media presentation from multiple related files [Figs. 7A-7C], including a control information file [i.e., the CDF; see col.1, lines 43-65] , stored on one or more server computers within a computer network [Figs.1 and 10; note that (i) in the case of off-line browsing the host computer (16, Fig.1) functions as a server with respect to the mobile device (18, Fig.1) and (ii) in the case of on-line browsing, the content provider functions as a server and the mobile device a client (see 12, 18, Fig.10)], the method comprising:

downloading the control information file to the client device [col.3, lines 21-32 and 50-56];

the client device parsing the control information file, wherein the control information file is an XML file [i.e., by default the CDF file is parsed by the receiving client's browser because it is written in XML format].

McLain teaches that the CDF file may contain a list of sound files for retrieving and rendering at the client device. McLain does not specifically teach that media presentation of an audio file and retrieval of its next file is performed concurrently.

However, in the same field of endeavor, White teaches a method for playing background music by playing an audio file and downloading its next file concurrently [1101, 1102, Fig.11B; col.14, lines 37-43].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to adopt the same concurrency in McLain's system because (1) audio clips need to be rendered in a smooth fashion and (2) by pipelining the retrieving and rendering process it would reduce transmission latency and avoid the burden of storing the entire set of audio clips locally [McLain: col.11, line 59 – col.12, line 23, wherein downloading files and filtering are performed in a streaming process].

17. As to claims 2-3, McLain further teaches that partitioning of media presentation information between the multiple related files is determined by information about the client and about the computer network [Abstract; col.11, lines 12-32; col.7, line 38 – col.8, line 36; note that since the receiving buffer of the mobile device is also part of the network, the capabilities of the mobile device are also part of the network parameters (e.g., communication bandwidth)].

18. As to claims 4-5, McLain further teaches that the media presentation comprises audio and/or video presentations [e.g., Figs. 7B-7C; col.10, line 61- col.11, line 9].

19. As to claim 6, McLain further teaches that partitioning of media presentation information between the multiple related files is described within the control information file using tags corresponding to respective files [col.3, lines 19-26, wherein XML uses tags to define various parameters (see also Table 1)].

20. As to claim 16, McLain further teaches that the XML file identifies multiple alternative files corresponding to a given segment of the media presentation [e.g., in terms of audio clips], further comprising selecting and retrieving one of the multiple alternative files [col.9, line 60 – col.10, line 34].

21. As to claims 12-13 and 17-22, since the features of these claims can also be found in claims 2-6 and 14-16, they are rejected for the same reasons set forth in the rejection of claims 2-6 and 14-16 above.

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Wecker et al.	[U.S. Pat. No. 6311058]; and
Wecker et al.	[U.S. Pat. No. 6449638].

23. Applicant's arguments with respect to claims 2-6 and 12-22 have been considered but are moot in view of the new ground(s) of rejection (see paragraph #6 of this office action).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Wen-Tai Lin whose telephone number is (703)305-4875. The examiner can normally be reached on Monday-Friday(8:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (703)305-9678. The fax phone numbers for the organization where this application or proceeding is assigned are as follows:

(703)746-7239 for official communications;

(703)746-7238 for after final communications; and

(703)746-5516 for status inquires draft communication.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-3900.

Wen-Tai Lin

September 30, 2004

Wen-Tai Lin
9/30/04

18

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

In re the Application

Inventor	**:**	**Shteyn**
Application No.	**:**	**09/433,257**
Filed	**:**	**November 4, 1999**
For	**:**	**PARTITIONING OF MP3 CONTENT FILE FOR EMULATING STREAMING**

APPEAL BRIEF

On Appeal from Group Art Unit 2154

Date: September 1, 2005

By: Michael Ure
Attorney for Applicant
Registration No. 33,089

Certificate of Fax/Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being faxed to ~~(703) 872-9306~~ (571) 273-8300. or deposited with the United States Postal Service as first class mail in an envelope addressed to the COMMISSIONER FOR PATENTS, Mail Stop Appeal, P.O. BOX 1450 ALEXANDRIA, VA 22313 on September 1, 2005.

Daniel Michalek
(Name)

01-Sep-05,
(Signature and Date)

TABLE OF CONTENTS

TABLE OF CASES

NONE

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the present application, Philips Electronics North America Corporation, and not the party named in the above caption.

II. RELATED APPEALS AND INTERFERENCES

With regard to identifying by number and filing date all other appeals or interferences known to Appellant which will directly effect or be directly affected by or have a bearing on the Board's decision in this appeal, Appellant is not aware of any such appeals or interferences.

III. STATUS OF CLAIMS

Claims 2-6 and 12-22 are pending, stand finally rejected, and form the subject matter of the present appeal.

IV. STATUS OF AMENDMENTS

All amendments have been entered. No amendment after final rejection has been submitted.

V. SUMMARY of the CLAIMED SUBJECT MATTER

The present invention relates to a flexible, client-driven method of media retrieval and presentation, as well as an intelligent client device for carrying out such method. In an exemplary embodiment, the method uses a parseable control information file such as an XML file. Media retrieval and presentation begins with retrieval and parsing of the control information file. A control script is then run by an XML interpreter, using output from the XML parser. In general, the control script retrieves files, or segments of the media presentation, from one or more server s in a computer network for sequential playout. Insofar as the particulars of which files are retrieved, when and from where, however, the control script offers great flexibility. For example, two or more alternative files may be provided corresponding to the same section of a media presentation, with the client device selecting between the alternatives based on device capability, for example, or network conditions, or other considerations.

Independent claim 14 relates to a method of, at a client device, forming a media presentation from multiple related files, including a control information file, stored on one or more server computers within a computer network. The control information file is downloaded to the client device. Based on parsing of the control information, the client device retrieves a first file and uses contents of the first file to being a media presentation, concurrent with the media presentation retrieves a next file, and uses content of the next file to continue the media presentation.

Independent claim 17 relates to a method of storing media presentation information within a computer network including multiple server computers. A control information file of a format to be parsed by a client device is stored on a server computer. Multiple related files accessible by the client device are stored on one or more server computers to, based on parsing of the control information file, form a media presentation from the multiple related files.

Independent claim 20 relates to a client device for forming a media presentation from multiple related files stored on server computers within a computer network. There are provided means for downloading files to the client device; means for parsing a control information file; and means for, based on parsing of the control information file, retrieving a first file and using contents of the first file to begin a media presentation, concurrent with the media presentation retrieving a next file, and using content of the next file to continue the media presentation.

VI. GROUNDS of REJECTION to be REVIEWED ON APPEAL

The issues in the present matter are whether:

1. claims 4-6 and 12-22 are unpatentable over Cohen in view of McLain.

VII. ARGUMENT

I. Rejection of Claims 4-6 and 12-22 as unpatentable over Cohen in view of McLain

Cohen relates to streaming of audio content. As described in column 6 of Cohen, clicking a link associated with the "connection file" of a desired media presentation causes an interactive display application—i.e., a proprietary media player--to be activated. The media player knows *a priori* the format of the connection file, which therefore need not be parsed. The connection file in Cohen is received and acted upon by the interactive display application, or media player (*not* a browser, for example). The connection file and the media player must be updated, if at all, in lock-step. The resulting system is rigid and inflexible.

The rejection states in part:

> Cohen taught the invention as substantially as claimed including ... the client device parsing the control information file [58, Fig. 5; col. 6, lines 26-40; i.e., the interactive display application program must parse the connection file in order to obtain the reference for segment file and its associated status]....
>
> * * *
>
> Cohen does not specifically teach how the connection file is formed and using what format.... However, McLain...teaches that the control information file may be written in the form of XML file and use the browser's parser for extracting parameters therein [McLain; see col. 1, lines 43-65].
>
> It would have been obvious...to have used XML as an alternative format for composing Cohen's connection file because XML is well known for its flexibility, with which it would make Cohen's connection file more dynamic and adaptable for containing the rather sophisticated file status information [col. 6, lines 26-40].

With respect to McLain, The system of McLain differs substantially from that of the claimed invention. McLain essentially teaches filtering content downloaded from an internet site according to a user profile for storage and use on a mobile device (i.e., offline browsing of internet content). The content may be downloaded to a PC and transferred to the mobile device, or may be downloaded directly to the mobile device. Regardless, in McLain, the content provider is not required to adapt to the system architecture by making available separate script files and data files. Hence McLain does not teach or suggest the salient feature of *downloading a control information file stored on a server computer*, parsing the same, and based on such parsing, retrieving (from a server) a first file to begin a media presentation, etc.; rather, McLain teaches away from this feature. There is no teaching or suggestion in McLain that the Channel Definition Format (CDF) file referred to in the background section is downloaded from the server preparatory to downloading content (e.g., segmented content) from the server.

The proposed combination of Cohen and McLain is the product of impermissible hindsight. There is nothing *in the references themselves* that would teach or suggest using XML for the connection file of Cohen.

More, particularly, Cohen makes no mention of XML or the supposed need for flexibility. McLain's teachings in regard to XML are simply that it may be used for purposes of a Channel Definition Format used to render content during offline browsing. Essentially, a CDF entry is created for each "qualifying" content element to be rendered on the mobile device, which may include both visual elements and audio elements. The CDF file is used to implement a filtering function.

The filtering concept for offline browsing of McLain, however, is not directly applicable to the streaming arrangement of Cohen. Streaming, of course, implies a continuous online connection. Furthermore, how techniques like those of McLain's might be applied to filtering a media presentation of the type contemplated in Cohen is not immediately apparent.

McLain itself does not so much as contain any teaching why XML is chosen for the CDF file.

Implicitly, then, the rationale for the rejection may be restated as follows: "Cohen does not teach the use of XML (or other format requiring parsing in accordance with the claims) for its connection file. XML was known at the time the invention was made, and was furthermore known to afford flexibility. Therefore it would have been obvious to use XML for the connection file of Cohen to achieve the flexibility offered by XML." One could just as well say that it would have been obvious to use XML for everything, in the name of flexibility, or that the use of XML constitutes an obvious "design choice." Such a statement does not satisfy the threshold of obviousness required under well-established precedent.

Accordingly, the Cohen and McLain references cannot be said to render obvious the inventions recited in claims 14, 17 and 20.

With regard to dependent claims 2-6, 12, 13, 15 and 16, dependent claims 18 and 19, and dependent claims 21 and 22, these claims depend from independent claims 14, 17 and 20, respectively, which have been shown to be patently distinguishable over the cited reference. Accordingly, these claims are also patently distinguishable and allowable over the cited references by virtue of their dependency upon an allowable base claims.

In view of the above, applicant submits that all of the above referred-to claims are patentable over the teachings of the cited references.

VIII. CONCLUSION

In view of the above analysis, it is respectfully submitted that the referenced teachings, whether taken individually or in combination, fail to anticipate or render obvious the subject matter of any of the present claims. Therefore, reversal of all outstanding grounds of rejection is respectfully solicited.

Date: September 1, 2005

By: Michael Ure
Attorney for Applicant
Registration No. 33,089

19

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Before the Board of Patent Appeals and Interferences

In re the Application

Inventor	**:**	**Shteyn**
Application No.	**:**	**09/433,257**
Filed	**:**	**November 4, 1999**
For	**:**	**PARTITIONING OF MP3 CONTENT FILE FOR EMULATING STREAMING**

APPEAL BRIEF

On Appeal from Group Art Unit 2154

Date: September 1, 2005

By: Michael Ure
Attorney for Applicant
Registration No. 33,089

Certificate of Fax/Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being faxed to (703) 872-9306 or deposited with the United States Postal Service as first class mail in an envelope addressed to the COMMISSIONER FOR PATENTS, Mail Stop Appeal, P.O. BOX 1450 ALEXANDRIA, VA 22313 on ______________.

VILMAIDA OACA
(Name)

8/18/06
(Signature and Date)

TABLE OF CONTENTS

TABLE OF CASES

NONE

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the present application, Philips Electronics North America Corporation, and not the party named in the above caption.

II. RELATED APPEALS AND INTERFERENCES

With regard to identifying by number and filing date all other appeals or interferences known to Appellant which will directly effect or be directly affected by or have a bearing on the Board's decision in this appeal, Appellant is not aware of any such appeals or interferences.

III. STATUS OF CLAIMS

Claims 2-6 and 12-22 are pending, stand finally rejected, and form the subject matter of the present appeal.

IV. STATUS OF AMENDMENTS

All amendments have been entered. No amendment after final rejection has been submitted.

V. SUMMARY of the CLAIMED SUBJECT MATTER

The present invention relates to a flexible, client-driven method of media retrieval and presentation, as well as an intelligent client device for carrying out such method. In an exemplary embodiment, the method uses a parseable control information file such as an XML file. Media retrieval and presentation begins with retrieval and parsing of the control information file. A control script is then run by an XML interpreter, using output from the XML parser. In general, the control script retrieves files, or segments of the media presentation, from one or more server s in a computer network for sequential playout. Insofar as the particulars of which files are retrieved, when and from where, however, the control script offers great flexibility. For example, two or more alternative files may be provided corresponding to the same section of a media presentation, with the client device selecting between the alternatives based on device capability, for example, or network conditions, or other considerations.

Independent claim 14 relates to a method of, at a client device, forming a media presentation from multiple related files, including a control information file, stored on one or more server computers within a computer network. The control information file is downloaded to the client device. Based on parsing of the control information, the client device retrieves a first file and uses contents of the first file to being a media presentation, concurrent with the media presentation retrieves a next file, and uses content of the next file to continue the media presentation.

Independent claim 17 relates to a method of storing media presentation information within a computer network including multiple server computers. A control information file of a format to be parsed by a client device is stored on a server computer. Multiple related files accessible by the client device are stored on one or more server computers to, based on parsing of the control information file, form a media presentation from the multiple related files.

Independent claim 20 relates to a client device for forming a media presentation from multiple related files stored on server computers within a computer network. There are provided means for downloading files to the client device; means for parsing a control information file; and means for, based on parsing of the control information file, retrieving a first file and using contents of the first file to begin a media presentation, concurrent with the media presentation retrieving a next file, and using content of the next file to continue the media presentation.

VI. GROUNDS of REJECTION to be REVIEWED ON APPEAL

The issues in the present matter are whether:

1. claims 4-6 and 12-22 are unpatentable over Cohen in view of McLain.

VII. ARGUMENT

I. Rejection of Claims 4-6 and 12-22 as unpatentable over Cohen in view of McLain

Cohen relates to streaming of audio content. As described in column 6 of Cohen, clicking a link associated with the "connection file" of a desired media presentation causes an interactive display application—i.e., a proprietary media player--to be activated. The media player knows *a priori* the format of the connection file, which therefore need not be parsed. The connection file in Cohen is received and acted upon by the interactive display application, or media player (*not* a browser, for example). The connection file and the media player must be updated, if at all, in lock-step. The resulting system is rigid and inflexible.

The rejection states in part:

> Cohen taught the invention as substantially as claimed including ... the client device parsing the control information file [58, Fig. 5; col. 6, lines 26-40; i.e., the interactive display application program must parse the connection file in order to obtain the reference for segment file and its associated status]....
>
> * * *
>
> Cohen does not specifically teach how the connection file is formed and using what format.... However, McLain...teaches that the control information file may be written in the form of XML file and use the browser's parser for extracting parameters therein [McLain; see col. 1, lines 43-65].
>
> It would have been obvious...to have used XML as an alternative format for composing Cohen's connection file because XML is well known for its flexibility, with which it would make Cohen's connection file more dynamic and adaptable for containing the rather sophisticated file status information [col. 6, lines 26-40].

With respect to McLain, The system of McLain differs substantially from that of the claimed invention. McLain essentially teaches filtering content downloaded from an internet site according to a user profile for storage and use on a mobile device (i.e., offline browsing of internet content). The content may be downloaded to a PC and transferred to the mobile device, or may be downloaded directly to the mobile device. Regardless, in McLain, the content provider is not required to adapt to the system architecture by making available separate script files and data files. Hence McLain does not teach or suggest the salient feature of *downloading a control information file stored on a server computer*, parsing the same, and based on such parsing, retrieving (from a server) a first file to begin a media presentation, etc.; rather, McLain teaches away from this feature. There is no teaching or suggestion in McLain that the Channel Definition Format (CDF) file referred to in the background section is downloaded from the server preparatory to downloading content (e.g., segmented content) from the server.

The proposed combination of Cohen and McLain is the product of impermissible hindsight. There is nothing *in the references themselves* that would teach or suggest using XML for the connection file of Cohen.

More, particularly, Cohen makes no mention of XML or the supposed need for flexibility. McLain's teachings in regard to XML are simply that it may be used for purposes of a Channel Definition Format used to render content during offline browsing. Essentially, a CDF entry is created for each "qualifying" content element to be rendered on the mobile device, which may include both visual elements and audio elements. The CDF file is used to implement a filtering function.

The filtering concept for offline browsing of McLain, however, is not directly applicable to the streaming arrangement of Cohen. Streaming, of course, implies a continuous online connection. Furthermore, how techniques like those of McLain's might be applied to filtering a media presentation of the type contemplated in Cohen is not immediately apparent.

McLain itself does not so much as contain any teaching why XML is chosen for the CDF file.

Implicitly, then, the rationale for the rejection may be restated as follows: "Cohen does not teach the use of XML (or other format requiring parsing in accordance with the claims) for its connection file. XML was known at the time the invention was made, and was furthermore known to afford flexibility. Therefore it would have been obvious to use XML for the connection file of Cohen to achieve the flexibility offered by XML." One could just as well say that it would have been obvious to use XML for everything, in the name of flexibility, or that the use of XML constitutes an obvious "design choice." Such a statement does not satisfy the threshold of obviousness required under well-established precedent.

Accordingly, the Cohen and McLain references cannot be said to render obvious the inventions recited in claims 14, 17 and 20.

With regard to dependent claims 2-6, 12, 13, 15 and 16, dependent claims 18 and 19, and dependent claims 21 and 22, these claims depend from independent claims 14, 17 and 20, respectively, which have been shown to be patently distinguishable over the cited reference. Accordingly, these claims are also patently distinguishable and allowable over the cited references by virtue of their dependency upon an allowable base claims.

In view of the above, applicant submits that all of the above referred-to claims are patentable over the teachings of the cited references.

VIII. CONCLUSION

In view of the above analysis, it is respectfully submitted that the referenced teachings, whether taken individually or in combination, fail to anticipate or render obvious the subject matter of any of the present claims. Therefore, reversal of all outstanding grounds of rejection is respectfully solicited.

Date: September 1, 2005

By: Michael Ure
Attorney for Applicant
Registration No. 33,089

20

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/433,257	11/04/1999	YEVGENIY EUGENE SHTEYN	PHA-23.782	2314

24737 7590 06/24/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
LIN, WEN TAI	
ART UNIT	PAPER NUMBER
2154	
MAIL DATE	DELIVERY MODE
06/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/433,257	**Applicant(s)** SHTEYN, YEVGENIY EUGENE	
	Examiner Wen-Tai Lin	**Art Unit** 2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 May 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-6 and 12-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-6 and 12-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 2-6 and 12-22 are presented for examination.

2. The text of those sections of Title 35, USC code not included in this action can be found in the prior Office Action.

Claim Rejections - 35 USC § 103

3. Claims 4-6 and 12-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen [U.S. Pat. No. 5751968] in view of McLain [U.S. Pat. No. 6493758].

4. Cohen was cited in the previous office action.

5. As to claims 14-15, Cohen teaches the invention substantially as claimed including: a method of, at a client device, forming a media presentation from multiple related files, including a control information file [54, Fig.5; col.6, lines 26-40], stored on one or more server computers within a computer network, the method comprising:

downloading the control information file to the client device [56, Fig.5];

the client device parsing the control information file [58, Fig.5; col.6, lines 26-40; i.e., the interactive display application program must parse the connection file in order to obtain the reference for segment file and its associated status]; and

based on the control information file, the client device:

retrieving a first file and using contents of the first file to begin a media presentation [60, Fig.5; col.6, lines 41-44];

concurrent with the media presentation, retrieving a next file; and

using content of the next file to continue the media presentation [64, Fig.5; col.6, lines 44-54].

Cohen does not specifically teach how the connection file is formed and using what format. That is, Cohen does not indicate whether the parameters contained in the control information file are extracted via parsing or not. However, in the same field of endeavor, McLain teaches that the control information file may be written in the form of XML file and use the browser's parser for extracting parameters therein [McLain: see col.1, lines 43-65].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have used XML as an alternative format for composing Cohen's connection file because XML is well known for its flexibility, with which it would make Cohen's connection file more dynamic and adaptable for containing the rather sophisticated file status information [col.6, lines 26-40].

6. As to claims 4-5, Cohen further teaches that the media presentation comprises an audio presentation or a video presentation [col.1, lines 49-54].

7. As to claim 6, Cohen in view of McLain teaches that partitioning of media presentation information between the multiple related files is described within the control information file

using tags corresponding to respective files [i.e., XML uses tags for specifying various parameters and values].

8. As to claim 16, Cohen in view of McLain further teaches that the XML file identifies multiple alternative files corresponding to a given segment of the media presentation, the method further comprising selecting and retrieving one of the multiple alternative files [Cohen: col.6, line 63 – col.7, line 5].

9. As to claims 12-13 and 17-22, since the features of these claims can also be found in claims 4-6 and 14-16, they are rejected for the same reasons set forth in the rejection of claims 4-6 and 14-16 above.

10. Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen [U.S. Pat. No. 5751968], as applied to claims 4-6 and 12-22 above and McLain [U.S. Pat. No. 6493758], as applied to claims 4-6 and 12-22 above, further in view of Lin et al.(hereafter "Lin")[U.S. Pat. No. 6405256].

11. Lin was cited from the previous office action.

12. As to claim 2, Cohen does not specifically teach that partitioning of media presentation information between the multiple related files is determined by information about the client.

However, Lin teaches a data streaming method/system wherein partitioning of streamed data is based on the buffering capability of the client device [Lin: col.6, lines 47-50]. It would have been obvious to one of ordinary skill in the art at the time the invention was made that Cohen's data file size should be a factor of the client's buffering and display capability because this criterion makes sure that data streaming in Cohen's media presentation can be achieved without overflowing the client's buffering capacity [col.5, lines 39-53].

13. As to claim 3, Cohen does not specifically teach that partitioning of media presentation information between the multiple related files is determined by information about the computer network.

However, Lin teaches a network comprising a plurality of caching servers, each with expandable buffer for storing additional segments of streamed data for absorbing network congestion [Abstract]. Since the caching servers and the network congestion are part of the information of the network, it is obvious that the data segmentation in Cohen's network, which obviously also comprises a plurality of communication nodes, should also be based on the network's buffering capability in each intermediate network node, because by doing so one would be able to anticipate Cohen system's tolerance against traffic fluctuation.

14. Claims 2-6 and 12-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over McLain [U.S. Pat. No. 6493758] in view of White et al. (hereafter "White") [U.S. Pat. No. 6005563].

15. As to claims 14-15, McLain teaches the invention substantially as claimed including: a method of, at a client device, forming a media presentation from multiple related files [Figs. 7A-7C], including a control information file [i.e., the CDF; see col.1, lines 43-65] , stored on one or more server computers within a computer network [Figs.1 and 10; note that (i) in the case of off-line browsing the host computer (16, Fig.1) functions as a server with respect to the mobile device (18, Fig.1) and (ii) in the case of on-line browsing, the content provider functions as a server and the mobile device a client (see 12, 18, Fig.10)], the method comprising:

downloading the control information file to the client device [col.3, lines 21-32 and 50-56];

the client device parsing the control information file, wherein the control information file is an XML file [i.e., by default the CDF file is parsed by the receiving client's browser because it is written in XML format].

McLain teaches that the CDF file may contain a list of sound files for retrieving and rendering at the client device. McLain does not specifically teach that media presentation of an audio file and retrieval of its next file is performed concurrently.

However, in the same field of endeavor, White teaches a method for playing background music by playing an audio file and downloading its next file concurrently [1101, 1102, Fig.11B; col.14, lines 37-43].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to adopt the same concurrency in McLain's system because (1) audio clips need to be rendered in a smooth fashion and (2) by pipelining the retrieving and rendering process it would reduce transmission latency and avoid the burden of storing the entire set of audio clips locally

[McLain: col.11, line 59 – col.12, line 23, wherein downloading files and filtering are performed in a streaming process].

16. As to claims 2-3, McLain further teaches that partitioning of media presentation information between the multiple related files is determined by information about the client and about the computer network [Abstract; col.11, lines 12-32; col.7, line 38 – col.8, line 36; note that since the receiving buffer of the mobile device is also part of the network, the capabilities of the mobile device are also part of the network parameters (e.g., communication bandwidth)].

17. As to claims 4-5, McLain further teaches that the media presentation comprises audio and/or video presentations [e.g., Figs. 7B-7C; col.10, line 61- col.11, line 9].

18. As to claim 6, McLain further teaches that partitioning of media presentation information between the multiple related files is described within the control information file using tags corresponding to respective files [col.3, lines 19-26, wherein XML uses tags to define various parameters (see also Table 1)].

19. As to claim 16, McLain further teaches that the XML file identifies multiple alternative files corresponding to a given segment of the media presentation [e.g., in terms of audio clips], further comprising selecting and retrieving one of the multiple alternative files [col.9, line 60 – col.10, line 34].

20. As to claims 12-13 and 17-22, since the features of these claims can also be found in claims 2-6 and 14-16, they are rejected for the same reasons set forth in the rejection of claims 2-6 and 14-16 above.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Wen-Tai Lin whose telephone number is (571) 272-3969. The examiner can normally be reached on Monday-Friday(8:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone numbers for the organization where this application or proceeding is assigned are as follows:

(703)746-7239 for official communications;

(703)746-7238 for after final communications; and

(703)746-5516 for status inquires draft communication.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-3900.

Wen-Tai Lin

June 19, 2008

/Wen-Tai Lin/

Primary Examiner, Art Unit 2154

21

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	Atty. Docket: PHA 23,782
YEVGENIY EUGENE SHTEYN	Group Art Unit: 2154
Serial No.: 09/433,257	Examiner: WEN TAI LIN
Filed: NOVEMBER 4, 1999	CONF. NO.: 2314

TITLE: PARTITIONING OF MP3 CONTENT FILE FOR EMULATING STREAMING

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

Sir:

In response to the Office Action of June 24, 2008, please amend the application and consider the remarks as follows:

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

2. (Previously presented) The method of claim 14, wherein partitioning of media presentation information between the multiple related files is determined by information about the client.

3. (Previously presented) The method of claim 14, wherein partitioning of media presentation information between the multiple related files is determined by information about the computer network.

4. (Previously presented) The method of claim 14, wherein the media presentation comprises an audio presentation.

5. (Previously presented) The method of claim 14, wherein the media presentation comprises a video presentation.

6. (Previously presented) The method of claim 14, wherein

partitioning of media presentation information between the multiple related files is described within the control information file using tags corresponding to respective files.

12. (Currently amended) The device of claim 18, wherein:
[[-]] the device interprets the control information to retrieve multiple files from the computer network for sequential play-out.

13. (Currently amended) The device of claim 12, wherein:
[[-]] the means for parsing comprises an XML parser; and
[[-]] the means for retrieving and using comprises an XML interpreter.

14. (Currently amended) A method of, at a client device, forming a media presentation from multiple related files, including a control information file, stored on one or more server computers within a computer network, the method comprising acts of:

downloading the control information file to the client device;

the client device parsing the control information file; and

based on parsing of the control information file, the client device:

identifying multiple alternative files corresponding to a given segment of the media presentation,

determining which file of the multiple alterative files to retrieve based on system constraints;

retrieving ~~a first file and using contents of the first file~~the determined file of the multiple alternative files to begin a media presentation~~;~~, wherein if the determined file is one of a plurality of files required for the media presentation, the method further comprising acts of:

concurrent with the media presentation, retrieving a next file; and

using content of the next file to continue the media presentation.

15. (Previously presented) The method of claim 14 wherein the control information file is an XML file.

16. (Currently amended) The method of claim 15, wherein the XML file identifies the multiple alternative files corresponding to ~~a~~ the given segment of the media presentation, further comprising an act of partitioning the media presentation into ~~selecting and~~

~~retrieving one of the multiple alternative files~~multiple MP3 files corresponding to a portion of the multiple alternative files.

17. (Currently amended) A method of storing media presentation information within a computer network including multiple server computers, the method comprising acts of:

storing on a server computer a control information file of a format to be parsed by a client device; and

storing on one or more server computers multiple ~~related~~ alternative files corresponding to a given segment of a media presentation accessible by the client device to, based on parsing of the control information file, determine which file of the multiple alterative files to retrieve based on system constraints to form a media presentation from the multiple ~~related~~ alternative files.

18. (Previously presented) The method of claim 17, wherein the control information file is an XML file.

19. (Currently amended) The method of claim 18, wherein the XML file identifies the multiple alternative files corresponding to ~~a~~

the given segment of the media presentation.

20. (Currently amended) A client device for forming a media presentation from multiple related files stored on server computers within a computer network, comprising:

means for downloading files to the client device;

means for parsing a control information file; and

means for parsing, based on parsing of the control information file:

identifying multiple alternative files corresponding to a given segment of the media presentation;

determining which file of the multiple alterative files to retrieve based on system constraints;

retrieving ~~a first file and using contents of the first file~~ the determined file of the multiple alternative files to begin a media presentation, wherein if the determined file is one of a plurality of files required for the media presentation, the means for parsing comprises means for;

concurrent with the media presentation, retrieving a next file; and

using content of the next file to continue the media presentation.

21. (Previously presented) The method of claim 20, wherein the control information file is an XML file.

22. (Currently amended) The method of claim 21, wherein the XML file identifies multiple alternative MP3 files corresponding to a portion of the given segment of the media presentation, the means for retrieving comprising means for selecting and retrieving one of the multiple alternative MP3 files.

REMARKS/ARGUMENTS

This Amendment is being filed in response to the Office Action dated June 24, 2008. Reconsideration and allowance of the application in view of the amendments made above and the remarks to follow are respectfully requested.

Claims 2-6 and 12-22 are pending in the Application.

In the Office Action, claims 4-6 and 12-22 are rejected under 35 U.S.C. §103(a) as allegedly unpatentable over U.S. Patent No. 5,751,968 to Cohen ("Cohen") in view of U.S. Patent No. 6,493,758 to McLain ("McLain"). Claims 2-3 are rejected under 35 U.S.C. §103(a) as allegedly being obvious over Cohen in view of McLain in further view of U.S. Patent No. 6,405,256 to Lin ("Lin"). Claims 2-6 and 12-22 are rejected under 35 U.S.C. §103(a) as allegedly being obvious over McLain in view of U.S. Patent No. 6,005,563 to White ("White"). These rejections are respectfully traversed. It is respectfully submitted that claims 2-6 and 12-22 are allowable over Cohen in view of McLain alone and in view of Lin and further that claims 2-6 and 12-22 are allowable over McLain in view of White for at least the following reasons.

It is undisputed that Cohen or White fails to teach "that the XML file identifies multiple alternative files corresponding to a given segment of the media presentation, the method further comprising selecting and retrieving one of the multiple alternative files ..." (See, Office Action, page 4, numbered paragraph 8, and page 7, numbered paragraph 19.) The Office Action relies in McLain for disclosing this feature, however, it is respectfully submitted that reliance on McLain is misplaced.

McLain shows a system for offline viewing of content with a mobile device. The sections of McLain cited in the Office Action for allegedly showing these features in fact merely describe common features of a networking environment (see, McLain, Col. 6, lines 65-66) including LAN, network interface and adapter (see, Col. 7, lines 1-5). While McLain does describe a downloading module (see, Col. 7 line 36 through Col. 8, line 17), the organization of files in McLain has nothing to do with the presently claimed methods and device. McLain describes that a file may be organized in a hierarchical manner (see, Col. 8, lines 6-12) and wherein user constraints on download size may limit the number of linked data portions of the hierarchy that are downloaded. However, as is readily appreciated, a hierarchical data structure such as discussed by McLain, has hierarchical portions that describe different parts of a presentation, not multiple alternative files corresponding to a given segment of the media presentation as recited in the claims.

It is respectfully submitted that the method of claim 14 is not made obvious by the teachings of Cohen in view of McLain and McLain in view of White. For example, Cohen in view of McLain and McLain in view of White does not disclose or suggest, a method that amongst other patentable elements, comprises (illustrative emphasis added) "based on parsing of the control information file, the client device: identifying multiple alternative files corresponding to a given segment of the media presentation, determining which file of the multiple alterative files to retrieve based on system constraints; retrieving the determined file of the multiple alternative files to begin a media presentation ..." as recited in claim 14, and as similarly recited in each of claims 17 and 20. Lin is introduced for allegedly showing elements of the dependent claims and as such, does nothing to cure the deficiencies in each of Cohen in view of McLain and McLain in view of White.

Based on the foregoing, the Applicant respectfully submits that independent claims 14, 17 and 20 are patentable over Cohen in view of McLain and McLain in view of White and notice to this effect is earnestly solicited. Claims 2-13, 15-16, 18-19 and 21-22 respectively depend from one of claims 14, 17 and 20 and accordingly are allowable for at least this reason as well as for the separately patentable elements contained in each of the claims. Accordingly, separate consideration of each of the dependent claims is respectfully requested.

In addition, Applicant denies any statement, position or averment of the Examiner that is not specifically addressed by the foregoing argument and response. Any rejections and/or points of argument not addressed would appear to be moot in view of the presented remarks. However, the Applicant reserves the right to submit further arguments in support of the above stated position, should that become necessary. No arguments are waived and none of the Examiner's statements are conceded.

Applicant has made a diligent and sincere effort to place this application in condition for immediate allowance and notice to this effect is earnestly solicited.

Respectfully submitted,

By Gregory L. Thorne

Gregory L. Thorne, Reg. 39,398
Attorney for Applicant(s)
September 23, 2008

THORNE & HALAJIAN, LLP
Applied Technology Center
111 West Main Street
Bay Shore, NY 11706
Tel: (631) 665-5139
Fax: (631) 665-5101

22

9/B
5-29-98
clm
(AE)
Enter
6-22-98
NP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of — Atty. Docket

LEONARDUS G.M. BEUK — PHN 15,180

Serial No. 08/601,140 — Group Art Unit: 2774

Filed: February 13, 1996 — Examiner: K. Chang

A PORTABLE DATA PROCESSING APPARATUS PROVIDED WITH A SCREEN AND A GRAVITATION-CONTROLLED SENSOR FOR SCREEN ORIENTATION

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

AMENDMENT UNDER RULE 116

Sir:

In response to the Final Rejection dated February 18, 1998, please amend the above-identified application under the provisions of 37 C.F.R. §1.116 as follows:

IN THE SPECIFICATION

Page 1, line 19, change "non-stationary" to --an acceleration based--;

line 20, change "non-stationary" to --acceleration based--;

Page 2, line 11, change "non-stationary" to --acceleration based--;

Page 4, line 1, after "orientation" insert --, such as by acceleration of the screen--;

B1

Page 5, line 2, delete "non-";

line 3, change "stationary" to --acceleration based, such as with respect to altering the motion

B2
cont

B2 cont'd

vector of the object with respect to speed or direction; after "orientation" insert --of the screen--.

IN THE ABSTRACT

Page 7, line 5, change "a non-stationary" to --an acceleration based--.

IN THE CLAIMS

Please amend the claims as follows:

C

1. (amended) A [portable] ~~manipulable~~ manipulatable apparatus having data processing means and [integrated] screen means for displaying one or more graphical or other objects presented by said data processing means, [said screen means having] a gravitation-controlled sensor means integrated with said screen means and feeding said data processing means for measuring an acceleration [a] [spatial orientation] of said screen means induced by user manipulation of the screen means, wherein said data processing means have programmed calculating means for under control of a [predetermined range of spatial orientations] screen motion sensed by said ~~sensing~~ sensor means imparting [a non-stationary] an acceleration based motion pattern to a predetermined selection among said objects.

B3 D

C

Claim 5, lines 1 and 2, delete "non-stationary".

Claim 6, lines 1 and 2, delete "non-stationary";
line 2, after "orientation" insert --of the screen means--.

Claim 7, lines 1 and 2, delete "non-stationary".

B4

8. (twice amended) An apparatus as Claim 1, wherein said motion represents a [transfer of an associated predetermined object between said screen means and a predetermined off-screen device] a motion of the object as if the force applied to the screen were applied to the object.

REMARKS

Claims 1-4 stand finally rejected 35 U.S.C. §102(e) as being anticipated by Donahue. In the previous amendment, Applicant argued the patentability of claim 1 on the basis that the orientation sensor in Donahue was separate from the screen means. However, the Examiner has pointed out at column 7, lines 51-57 that the sensor unit and the display can be incorporated into a single helmet, thereby negating Applicant's argument thereon.

It is respectfully noted, however, that a non-obvious distinction still exists between Donahue and the invention of the present application. In Figures 8 through 13, Donahue illustrates a tilt orientation sensor 22 which "operates in the principle of comparing orientation of the sensor to the Earth's gravitational field" (column 9, lines 12-16). Donahue's sensor includes a

S:\WI\PW15WIA0.RUR

10

weighted sphere which maintains a fixed orientation included in a fluid-filled housing which can rotate around this sphere. Also included are a light cone and optical sensors which measure the angle inclination of the housing relative to the sphere. While Donahue's sensor can measure tilt by measuring the angle of rotation of the housing about the sphere, it cannot measure acceleration as do the sensors in the present invention.

As described beginning a line 25 on page 3 of the specification, Applicant's sensor includes the sensing of a differential element such as with piezoelectricity or strain gauges. Further, as mentioned in the sentence bridging pages 3 and 4, the sensors can measure "dynamical changes of the spatial orientation", which of course indicate acceleration in direction or position. Additionally, the motion imparted in Applicant's device to the object based on the sensed acceleration is acceleration based. As described at page 5, lines 5-14, the object may "fall" under constant acceleration or "fly like a balloon", or otherwise accelerate with respect to position or direction as if influenced by a pseudo-forced exerted on the object on the screen or pseudo-gravity.

Thus, in the instant invention, because of the integration of the acceleration based sensor to the screen, an object displayed on the screen can be made to move as if the user's manipulation of the screen were instead manipulating the object. In contrast, this relationship cannot be obtained in Donahue's device, in which rotation or tilting of the sensor can be detected,

B

but not acceleration of the screen (in the case of integrated helmet). Accordingly, claim 1 has been amended herein to recite a manipulatable apparatus having a screen means with a gravitational controlled sensor integrated with the screen means and feeding the data processing means for measuring an acceleration of the screen means induced by user manipulation. The data processing means, under control of a screen acceleration motion sensed by the sensing means imparts an acceleration-based motion pattern to an object displayed on the screen.

It is noted that the term "non-stationary" has been changed to "acceleration based", as this term is more accurate with respect to the "pseudo-force" and "pseudo-gravity" motions described in the specification. The term "non-stationary" referred to non-stationary in time, also meaning "acceleration", but "acceleration" is more commonly used in art, so it has been adopted herein.

Additionally, claims 5-7 have been amended to remove the term "non-stationary" to ensure complete congruity with amended claim 1. Claim 8 has also been amended to recite that the motion of the object represents a motion as if the force applied to the screen were applied to the object, as described in the specification at page 5, lines 6-7.

For all of the above reasons, claim 1 and its dependent claims now clearly distinguish over Donahue, which does not show or suggest a manipulatable device having a screen and sensor integrated therewith which sensor senses an acceleration of the screen caused by user movement thereof, which is then used to impart an acceleration based motion to an object displayed on the screen.

The above revisions are believed to be properly enterable under the provisions of Rule 116 by placing the claims in condition for allowance. The claims are first presented at this time to overcome the Examiner's argument concerning Donahue's helmet embodiment which integrates the screen and sensor, which was first put forward by the Examiner in the Final Office Action. As discussed above, the revisions made herein clearly overcome Donahue's helmet based embodiment due to the differences in the capabilities of the sensor and the motions imparted to the object.

Accordingly, entry of the amendment, reconsideration of the rejections and allowance of all the claims are respectfully solicited. Also, enclosed for entry by the Examiner is a Notice of Appeal for the depending claims 1-10, which the Examiner is respectfully requested to enter should the Examiner maintain the Final Rejection.

Respectfully submitted,

By____________________
Brian J. Wieghaus, Reg. 32,603
Attorney
(914) 333-9633
May 18, 1998

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to:

COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

On May 18, 1998

By____________________
Brian J. Wieghaus, Reg. 32,603

S:\WI\PW15WIA0.RUR

23

GAU 2774

14/C
11-4-98
NP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of
LEONARDUS G.M. BEUK
Serial No. 08/601,140
Filed: February 13, 1996

Atty. Docket
PHN 15,180A
Group Art Unit: 2774
Examiner: K. Chang

A PORTABLE DATA PROCESSING APPARATUS PROVIDED WITH A SCREEN AND A GRAVITATION-CONTROLLED SENSOR FOR SCREEN ORIENTATION

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

AMENDMENT

Sir:

In response to the Office Action mailed August 18, 1998, please amend the above-identified application as follows:

IN THE CLAIMS

Please amend claim 1 and add new claim 11 as follows:

Claim 1, line 1, change "manipulable" to --manipulatable--.

C1 cont

11. A manipulatable apparatus having data processing means and a display screen for displaying one or more graphical or other objects presented by said data processing means, a gravitation-controlled sensor integrated with said display screen and feeding said data processing means for measuring dynamical changes of the spatial orientation of said display screen induced by user manipulation of the display screen, wherein said data processing means have programmed calculating means for under control of a screen motion sensed by said sensor, due to dynamical changes of

C1 concld

the spatial orientation of the screen, imparting an acceleration based motion pattern to a predetermined selection among said objects which motion corresponds to the dynamical change of the spatial orientation of the screen.

REMARKS

The amendment filed June 16, 1998 stands rejected to under 35 U.S.C. §132 as introducing new matter to the disclosure. The Examiner concludes that the added material which is not supported by the original disclosure is the measuring acceleration of screen means and induced by user manipulation of the screen means.

Applicant respectfully traverses the above objection on the grounds that the objection is a mere conclusion without any supporting rationale. Without any supporting rationale, it is impossible for Applicant to respond to the Examiner's objection in a meaningful way. Applicant respectfully notes that in the Remarks of the June 16th amendment, Applicant discussed where there was support in the specification as originally filed for the subject matter of the sensor's measuring the acceleration of the screen induced by user manipulation of the screen. It is also noted that MPEP Section 707 requires that, "notification of the reasons for rejection and/or objection together with such information as may be useful in judging the propriety of continuing the prosecution should be given." Additionally, MPEP Section 707.07(t) clearly indicates that omnibus rejections should be avoided because they are not informative. It is respectfully submitted that since the Applicant provided rationale in the Remarks describing why the

12

amendments to the specification and claims were supported in the original specification, that the Examiner's mere conclusory statement does not comply with the letter or spirit of patent examining procedure. Accordingly, it is respectfully submitted if the Examiner maintains the objection, that the Examiner provides specific reasons why the support noted by the Applicant in the specification is insufficient in supporting the amendments made to the specification and claims.

Additionally, Applicant respectfully submits that the objection to the specification and claims is in error for the following additional reasons. First, as noted in the previous amendment the sensors measure "gravitation force". It is respectfully submitted that the force imposed by gravitation is caused by acceleration, namely the gravitational acceleration. Additionally, inherently piezoelectric or strain gauges are suitable for measuring force. Force causes acceleration. Conversely, measuring force gives an indication of acceleration. Finally, the specification clearly states in the sentence bridging pages 3,4 that "facility could as well be provided for measuring dynamical changes of the spatial orientation". Thus, in addition to describing an embodiment in which merely the spatial orientation of a stationary screen is measured, the specification also envisioned an embodiment which measures the "dynamical changes of the spatial orientation". It is respectfully submitted that the spatial orientation cannot change "dynamically" unless it is accelerated. Thus, measuring "dynamical changes of the spatial orientation" measures acceleration. Accordingly, it is respectfully believed that the revisions to the specification and claims were fully supported by the specification as originally filed.

Additionally, new claim 11 is presented for examination which specifically includes the language from the specification namely, the "measuring dynamical changes of the spatial orientation". Accordingly, new independent claim 11 is clearly supported by the specification.

In addition to the reasons previously noted why Donahue does not teach or suggest the measurement of acceleration of the screen means, it is also respectfully noted that Donahue did not teach or suggest the specific acceleration based movements of an object on the display screen, controlled by user manipulation of the display screen. In particular, nowhere does Donahue suggest the imparting of an acceleration based motion to the object. While Donahue clearly suggests that a cursor can be controlled by tilting of the integrated helmet, and that objects can be moved by tilting of the helmet, it does not suggest a correspondence between the acceleration of the screen and movement of the object nor between the "measuring dynamical changes of the spatial orientation" of the screen and the acceleration or gravity based movement of an object. Thus, if the Examiner is to continue to apply Donahue against the claims, the Examiner is respectfully requested to provide evidence as to where Donahue suggests imparting an acceleration based movement to an object which corresponds to an acceleration of the display screen.

For the above reasons, it is respectfully believed that the Office Action is not in compliance with the noted provisions of the MPEP. Accordingly, issuance of a new non-final Office Action is respectfully requested. Alternatively, it is respectfully submitted that the revisions to the specification and claims presented in the last Office Action are fully supported by the specification as originally filed, and withdrawal of the objection to the specification and claims on this ground is respectfully requested. Additionally, for all the reasons noted above the claims are correct both with respect to form and in distinguishing over Donahue. Accordingly entry of the amendment, reconsideration of the outstanding rejections/objections, and receipt of a Notice of Allowance is respectfully requested.

Respectfully submitted,

By Brian Wieghaus

Brian J. Wieghaus, Reg. 32,603
Attorney
(914) 333-9633
October 21, 1998

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to:

COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

On October 22, 1998

By Brian Wieghaus
Brian J. Wieghaus, Reg. 32,603

24

UNITED STATES .PARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/601,140	02/13/96	BEUK L	PHN-15.180

LM51/0112

CORPORATE PATENT COUNSEL
U S PHILIPS CORP
580 WHITE PLAINS ROAD
TARRYTOWN NY 10591

EXAMINER	
CHANG,K	
ART UNIT	**PAPER NUMBER**
2774	15

DATE MAILED: 01/12/99

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

PTO-90C (Rev. 2/95)
*U.S. GPO: 1998-437-638/80022

1- File Copy

Notice of Allowability	Application No. 08/601,140	Applicant(s) BEUK
	Examiner Kent Chang	Group Art Unit 2774

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance and Issue Fee Due or other appropriate communication will be mailed in due course.

☒ This communication is responsive to *the Amendment filed on 10/26/98*.

☒ The allowed claim(s) is/are *1-11*.

□ The drawings filed on ______________ are acceptable.

☒ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☒ All □ Some* □ None of the CERTIFIED copies of the priority documents have been

☒ received.

□ received in Application No. (Series Code/Serial Number) ______________.

□ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: ______________.

□ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

A SHORTENED STATUTORY PERIOD FOR RESPONSE to comply with the requirements noted below is set to EXPIRE **THREE MONTHS** FROM THE "DATE MAILED" of this Office action. Failure to timely comply will result in ABANDONMENT of this application. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

□ Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL APPLICATION, PTO-152, which discloses that the oath or declaration is deficient. A SUBSTITUTE OATH OR DECLARATION IS REQUIRED.

☒ Applicant MUST submit NEW FORMAL DRAWINGS

□ because the originally filed drawings were declared by applicant to be informal.

□ including changes required by the Notice of Draftsperson's Patent Drawing Review, PTO-948, attached hereto or to Paper No. _____.

☒ including changes required by the proposed drawing correction filed on *Dec 8, 1997*, which has been approved by the examiner.

□ including changes required by the attached Examiner's Amendment/Comment.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the reverse side of the drawings. The drawings should be filed as a separate paper with a transmittal lettter addressed to the Official Draftsperson.

□ Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Any response to this letter should include, in the upper right hand corner, the APPLICATION NUMBER (SERIES CODE/SERIAL NUMBER). If applicant has received a Notice of Allowance and Issue Fee Due, the ISSUE BATCH NUMBER and DATE of the NOTICE OF ALLOWANCE should also be included.

Attachment(s)

□ Notice of References Cited, PTO-892

□ Information Disclosure Statement(s), PTO-1449, Paper No(s). ________

□ Notice of Draftsperson's Patent Drawing Review, PTO-948

□ Notice of Informal Patent Application, PTO-152

□ Interview Summary, PTO-413

□ Examiner's Amendment/Comment

□ Examiner's Comment Regarding Requirement for Deposit of Biological Material

□ Examiner's Statement of Reasons for Allowance

RICHARD A. HJERPE
SUPERVISORY PATENT EXAMINER
GROUP 2700

25

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR		ATTORNEY DOCKET NO.
08/601,140	02/13/96	BEUK	L	PHN-15.180

LM61/0505

CORPORATE PATENT COUNSEL
U S PHILIPS CORP
580 WHITE PLAINS ROAD
TARRYTOWN NY 10591

EXAMINER	
CHANG, K	

ART UNIT	PAPER NUMBER
2774	18

DATE MAILED: 05/05/99

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

PTO-90C (Rev. 2/95)

1- File Copy

Response to Rule 312 Communication	Application No. 08/601,140	Applicant(s) BEUK
	Examiner KENT CHANG	Group Art Unit 2778

□ The petition filed on ________________ under 37 CFR 1.312(b) is granted. The paper has been forwarded to the examiner for consideration on the merits.

☒ The amendment filed on *Apr 15, 1999* under 37 CFR 1.312 has been considered, and has been:

□ entered.

☒ entered as directed to matters of form not affecting the scope of the invention (Order 3311).

□ disapproved. See explanation below.

□ entered in part. See explanation below.

Bipin H. Shalwala
Primary Examiner

26

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/508,917	07/24/2009	Francisciscus Lucas Antonius Johannes KAMPERMAN	NL020681US2	8927

24737 7590 10/28/2010
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
10/28/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 12/508,917	**Applicant(s)** KAMPERMAN, FRANCISCUS LUCAS ANTONIUS JO	
	Examiner DARREN SCHWARTZ	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _24 July 2009_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _14-22_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _14-22_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _24 July 2009_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Via a preliminary amendment, claims 1-13 are cancelled. Claims 14-22 are newly presented. Claims 14-22 are presented for examination.

Examiner's Remarks

In analyzing the claims under 35 U.S.C. 101, the Examiner notes claim 14 necessarily requires a machine as to calculate a distance between two communication devices, wherein the distance reflects a physical distance between said communication devices.

Claim Objections

Claim 22 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim, or amend the claim to place the claim in proper dependent form, or rewrite the claim in independent form.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 14 and 20-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey.

Re claim 14: Willey teaches a method of determining whether multimedia data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of

performing a distance measurement between the first communication device and the second communication device (Fig 11, elts 200 & 1010; Fig 11a, elts 46 & 48; ¶71; ¶76),

wherein the first and the second communication device share a common secret (Fig 5A; ¶49) which is used to perform the distance measurement and which has been shared before performing the distance measurement (Fig 5A; ¶3; ¶37; ¶49; Fig 11A, elts 40, 42, 44 & 46), the method further comprising the steps of:

performing an authentication check from the first communication device on the second communication device by checking whether the second communication device is compliant with a set of predefined compliance rules (¶56-¶58; *instances of values are exchanged and respectively validated between the two devices*);

sharing the common secret with the second communication device if the second communication device is compliant (¶56-¶58; *after the exchanged digits are validated, the key agreement proceeds*); and

using the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the multimedia data is transmitted from the first communication device to the second communication device (Fig 11a, elts 48 & 50).

Re claim 20: Willey teaches the step of sharing said common secret comprises executing one of a key transport protocol and a key agreement protocol (Fig 5A, elts 3, 4, 5 & 7).

Re claim 21: Claim 21 is rejected under similar rationale as those expressed as per claim 14 stated *supra*.

Re claim 22: Willey teaches a system for secure transfer of content comprising a first communication device as claimed in claim 21 (see Willey as applied to claim 14) and a second communication device (Fig 11, elt 1010) comprising means for playing back the multimedia data (¶35).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 15, 16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist.

Re claim 15: Willey teaches all the limitations of claim 14 as previously stated.

However, Lundkvist teaches:

transmitting a first signal from the first communication device [Fig 1, elt 1] to the second communication device [Fig 1, elt 1] at a first time t1, the second communication device being adapted for receiving the first signal (Fig 2, elts "Message x is determined and X is sent," –X→, "X is received and decrypted;" ¶32);

generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal to the first device (Fig 2, elts "X is received and decrypted" & "f(x) and is determined and Y1 is sent;" ¶32);

receiving the second signal at a second time t2 (Fig 2, elts: "←Y1—" and "Y1 is received, decrypted, f(x) and T1 are checked;" ¶32);

checking if the second signal has been modified according to the common secret (Fig 2, elt: "Y1 is received, decrypted, f(x) and T1 are checked;" ¶32); and

determining (323) the distance between the first and the second communication device according to a time difference between t1 and t2 (¶11; ¶20; ¶42; ¶53).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey with the teachings of Lundkvist, for the purpose of simultaneously validating & authenticating the credentials between two devices and the physical distance between said two devices; while Willey does these events sequentially, Lundkvist provides for these events simultaneously and is thus more efficient.

<u>Re claim 16</u>: The combination of Willey and Lundkvist teaches the first signal is a spread spectrum signal (Willey: ¶2; ¶83).

<u>Re claim 18</u>: The combination of Willey and Lundkvist teaches the first signal and the common secret are bit words and where the second signal comprises information being generated by performing an XOR between the bit words (Willey: ¶72-¶73).

3. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, in further view of Caputo et al (U.S. Pat 5778071 A), hereinafter referred to as Caputo.

Re claim 17: The combination of Willey and Lundkvist teaches all the limitations of 15 as previously stated.

However, Caputo teaches the step of checking [Fig 5A, elt 64] if the second signal [Fig 5A, elts 66 & 68] has been modified according to the common secret [Fig 5A, elts 62 & 70] comprises the steps of:

generating a third signal [Fig 5A, elts 55 & 62] by modifying the first signal [Fig 5A, elt 54] according to the common secret [Fig 5A, elts 63 & 69] and comparing the third signal [Fig 5A, elts 55 & 62] with the received second signal [Fig 5A, elts 64, 66 & 68] (col 13, line 25 – col 14, line 5).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey and Lundkvist with the teachings of Caputo, for the purpose of validating the occurrence of exchanged data without manipulated the actual data. Comparing signals without modification results in faster authentication than to decrypt subsequent validation.

4. Claims 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Simon et al (U.S. Pat 5937065 A), hereinafter referred to as Simon.

Re claim 19: Willey teaches all the limitations of claim 14 as previously stated.

However, Simon teaches wherein the authentication check further comprises the step of checking if the identification of the second device is compliant with an expected identification (Fig 3, elts 72, 73, 76 & 80; col 6, lines 36-50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey with the teachings of Simon, for the purpose of validating the devices themselves to prevent man-in-the-middle attacks or spoofing.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 14-19 and 21 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 3, 5-8 and 11 of copending Application No. 10/521858. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

Re instant claim 14:

Instant claim 14	Copending claim 6 (which encompasses the limitations of independent claim 1)
A first communication device configured for determining whether multimedia data stored on the first communication device are to be accessed by a second communication device, the device comprising means for performing distance measurement between the first	A method for a first communication device to performing authenticated distance measurement between said first communication device and a second communication device, wherein the first and the second communication device share a common secret and wherein the

communication device and the second communication device, wherein the first communication device comprises a memory storing a common secret also stored on the second communication device, which secret is used in performing the distance measurement, the first communication device being configured for sharing the common secret before performing the distance measurement, wherein the first communication device further comprises means for:	authenticated distance measurement comprises …
performing an authentication check on the second communication device, by checking whether the second communication device is compliant with a set of predefined compliance rules;	performing an authentication check from the first communication device on the second communication device, by checking whether said second communication device is compliant with a set of a predefined compliance rules;
sharing the common secret with the second communication device if the second communication device is compliant; and	if the second communication device is compliant, sharing said common secret by transmitting said secret to the second communication device,

using the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel.	wherein the common secret has been shared before performing the distance measurement.

The first and second communication devices are synonymous with one-another between the instant and copending claim; this is further held in the distance measurement, common secret and compliance rules.

However, the copending claim does not expressly disclose and transmitting multimedia data from the first communication device to the second communication device over the secure authenticated channel.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of the instant claim with the teachings of the copending claim, for the purpose of providing a communications service amongst devices that have mutually authenticated one another; mutual authentication is well known in the art prior to engaging in some form of communication in order to identify and protect both parties.

Re instant claim 15:

Instant claim 15	Copending claim 6 (which encompasses the limitations of independent claim 1)
transmitting a first signal from the first communication device to the second	wherein the authenticated distance measurement comprises: transmitting a

communication device at a first time t1, the second communication device being adapted for receiving the first signal;	first signal from the first communication device to the second communication device at a first time t1, said second communication device being adapted for receiving said first signal;
generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal to the first device;	generating a second signal by modifying the received first signal according to the common secret, and transmitting the second signal to the first communication device;
receiving the second signal at a second time t2;	receiving the second signal at a second time t2;
checking if the second signal has been modified according to the common secret; and	generating by the first communication device a third signal by modifying the first signal according to the common secret; comparing the third signal with the received second signal to check if the second signal has been modified according to the common secret; and
determining the distance between the first and the second communication device according to a time difference between t1	determining the distance between the first and the second communication device according to a time difference between t1

and t2.	and t2.

Re instant claim 16: Instant claim 16 is rejected as similar in scope to claim 3

Re instant claim 17: Instant claim 17 is rejected as similar in scope to claim 6.

Re instant claim 18: Instant claim 18 is rejected as similar in scope to claim 5.

Re instant claim 19: Instant claim 19 is rejected as similar in scope to claim 7.

Re instant claim 21: Instant claim 21 is rejected under provisional obviousness-double patenting as it pertains to copending claims 1, 6 & 11.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claims 20 and 22 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 6 of copending Application No. 10/521858 in view of Willey (U.S. Pat App Pub 2003/0065918 A1).

Re instant claim 20: Instant claim 14 with respect to copending claim 6 has been addressed supra. However, Willey teaches the step of sharing said common secret comprises executing one of a key transport protocol and a key agreement protocol (Fig 5a, elts 3, 4, 5 & 7; ¶40).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of copending claim 6 with the teachings of Willey, for the purpose of securely negotiating a key between two communication devices; Diffie-Hellman is known in the art as secure key agreement protocol.

Re instant claim 22: Instant claim 22 with respect to copending claim 6 has been addressed supra. However, Willey teaches a second communication device comprising means for playing back the multimedia data (¶35).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of copending claim 11 with the teachings of Willey, for the purpose of expanding the device functionality to present multimedia data; one of ordinary skill can appreciate incorporating into a portable device means for presenting multimedia data.

This is a provisional obviousness-type double patenting rejection.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 7am-5pm EST, Monday-Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435

27

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/508,917	07/24/2009	Franciscus Lucas Antonius Johannes KAMPERMAN	NL020681US2	8927

24737 7590 02/17/2011
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
02/17/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

Office Action Summary	**Application No.** 12/508,917	**Applicant(s)** KAMPERMAN, FRANCISCUS LUCAS ANTONIUS JO	
	Examiner Darren B. Schwartz	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _25 January 2011_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _14,15 and 17-22_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _14,15 and 17-22_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Applicant amends claims 14, 21 and 22. Applicant cancels claim 16.

Claims 14, 15 and 17-22 are presented for examination.

Response to Arguments

1. In light of Applicant's amendments to the claims, the claim objection is withdrawn.

Applicant's arguments with respect to claims 14, 15 and 17-22 have been considered but are moot in view of the new grounds of rejection.

2. Applicant argues on page 8 of Remarks: "Willey, however, fails to provide any teaching regarding the second device being compliant with predefined compliance rules. Rather Willey merely teaches that the devices are capable of communicating with one another and that after determining they may be paired together and are within a predetermined distance, the devices may exchange multimedia data."

The Examiner disagrees. In analyzing the claim language for what Applicant regards as "compliant with predefined compliance rules." While Applicant's disclosure of the invention provides an example of compliance, no explicit nor specific definition is defined; thus, the Examiner relies upon the ordinary meaning. The definition of "compliance" is: the act or process of complying to a desire, demand, or proposal; conformity in fulfilling official requirements. The Examiner cited ¶56-¶58 as the user of both pairing devices verifies the presentation of three digits from both devices; once verified by the user, a key agreement is established. Thus, this pairing procedure teaches checking whether the second communication device is compliant with a set of predefined compliance rules, wherein a set of predefined compliance rules is the verification of the three digits. The verification of these digits meets the claimed "compliance." Since both devices are mutually authenticated using these presented digits, both the first and second communication devices are verified for such compliance.

The Examiner indicates that while Applicant is argues Willey teaches away from the claimed compliance, Applicant fails to address what Applicant regards as compliance.

All of the disclosures in a reference must be evaluated for what they fairly teach one of ordinary skill in the art. "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Lemelson, 397 F.2d 1006, 1009 (CCPA 1968) (citing In re Boe, 355 F.2d 961, 965 (CCPA 1966).

The Examiner further notes the breadth of independent claims 14 and 21 which respectively recite "the second device being compliant with predefined compliance rules," yet, newly presented claim 22 recites "the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device." Thus, the claimed compliancy of claims 14 and 21 may be broadly construed as merely confirming a desired PIN code as the broad definition of compliancy is met.

The Examiner in no way confirms nor dissents upon Applicant's interpretation of the teachings of Willey and Lundkvist.

3. Applicant states on page 11 of Remarks: "With regard to the rejection of the claims under the doctrine of non-obvious double patenting, applicant respectfully requests that this rejection be held in abeyance until such time that either the instant application or the mentioned application issues, and then the issued claims may be compared to the claims of the remaining application to determine whether the rejection is still applicable."

Accordingly, the claim rejections are sustained. As necessitated by Applicant's amendments to the claims, a new grounds of rejection under non-obvious double patenting is supplied *infra*.

As necessitated by Applicant's amendments to the claims, the Examiner introduces Rofheart et al (U.S. Pat App Pub 2005/0265503 A1) and Overy et al (U.S. Pat App Pub 2003/0220765 A1).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 14, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart.

Re claim 14: Willey teaches a method of determining whether multimedia data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of

performing a distance measurement between the first communication device and the second communication device (Fig 11, elts 200 & 1010; Fig 11a, elts 46 & 48; ¶71; ¶76),

wherein the first and the second communication device share a common secret (Fig 5A; ¶49) which has been shared before performing the distance measurement (Fig 5A; ¶3; ¶37; ¶49; Fig 11A, elts 40, 42, 44 & 46), the method further comprising the steps of:

performing an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with a set of predefined compliance rules (¶56-¶58; *instances of values are exchanged and respectively validated between the two devices*);

sharing the common secret with the second communication device if the second communication device is compliant (¶56-¶58; *after the exchanged digits are validated, the key agreement proceeds*); and

using the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the multimedia data is transmitted from the first communication device to the second communication device (Fig 11a, elts 48 & 50).

However, Willey does not expressly disclose the common secret being used to modify the spreading code of a spread-spectrum communication signal between the first device and the second device.

Yet, Rofheart teaches the common secret being used to modify the spreading code of a spread-spectrum communication signal between the first device and the second device (¶67; ¶97; ¶159-¶160).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey with the spread-spectrum communication signals of Rofheart, for the purpose of providing secured communication between two parties wherein the secured communication is resistant from jamming; spread-spectrum signals have the known utility of providing secure communication resistant to natural interference and jamming.

It is further held that it would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute the asymmetric cipher of Rofheart with the symmetric cipher of Willey as symmetric ciphers are faster and not computer process intensive.

Re claim 20: Willey teaches the step of sharing said common secret comprises executing one of a key transport protocol and a key agreement protocol (Willey: Fig 5A, elts 3, 4, 5 & 7).

Re claim 21: Claim 21 is rejected under similar rationale as those expressed as per claim 14 stated *supra*.

5. Claims 15 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, in further view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist.

Re claim 15: The combination of Willey and Rofheart teaches all the limitations of claim 14 as previously stated.

However, Lundkvist teaches:

transmitting a first signal from the first communication device [Fig 1, elt 1] to the second communication device [Fig 1, elt 1] at a first time t1, the second communication device being adapted for receiving the first signal (Fig 2, elts “Message x is determined and X is sent,” –X→, “X is received and decrypted;” ¶32);

generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal to the first device (Fig 2, elts “X is received and decrypted” & "f(x) and is determined and Y1 is sent;" ¶32);

receiving the second signal at a second time t2 (Fig 2, elts: “←Y1—" and "Y1 is received, decrypted, f(x) and T1 are checked;" ¶32);

checking if the second signal has been modified according to the common secret (Fig 2, elt: “Y1 is received, decrypted, f(x) and T1 are checked;" ¶32); and

determining (323) the distance between the first and the second communication device according to a time difference between t1 and t2 (¶11; ¶20; ¶42; ¶53).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey and Rofheart with the teachings of Lundkvist, for the purpose of simultaneously validating & authenticating the credentials between two devices and the physical distance between said two devices; while Willey does these events sequentially, Lundkvist provides for these events simultaneously and is thus more efficient.

Re claim 18: The combination of Willey, Rofheart and Lundkvist teaches the first signal and the common secret are bit words and where the second signal comprises information being generated by performing an XOR between the bit words (Willey: ¶72-¶73).

6. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, Rofheart et al

(U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, and Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, in further view of Caputo et al (U.S. Pat 5778071 A), hereinafter referred to as Caputo.

Re claim 17: The combination of Willey, Rofheart and Lundkvist teaches all the limitations of 15 as previously stated.

However, Caputo teaches the step of checking [Fig 5A, elt 64] if the second signal [Fig 5A, elts 66 & 68] has been modified according to the common secret [Fig 5A, elts 62 & 70] comprises the steps of:

generating a third signal [Fig 5A, elts 55 & 62] by modifying the first signal [Fig 5A, elt 54] according to the common secret [Fig 5A, elts 63 & 69] and comparing the third signal [Fig 5A, elts 55 & 62] with the received second signal [Fig 5A, elts 64, 66 & 68] (col 13, line 25 – col 14, line 5).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey, Rofheart and Lundkvist with the teachings of Caputo, for the purpose of validating the occurrence of exchanged data without manipulated the actual data. Comparing signals without modification results in faster authentication than to decrypt subsequent validation.

7. Claims 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, in further view of Simon et al (U.S. Pat 5937065 A), hereinafter referred to as Simon.

Re claim 19: The combination of Willey and Rofheart teaches all the limitations of claim 14 as previously stated.

However, Simon teaches wherein the authentication check further comprises the step of checking if the identification of the second device is compliant with an expected identification (Fig 3, elts 72, 73, 76 & 80; col 6, lines 36-50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey with the teachings of Simon, for the purpose of validating the devices themselves to prevent man-in-the-middle attacks or spoofing.

8. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, in further view of Overy et al (U.S. Pat App Pub 2003/0220765 A1), hereinafter referred to as Overy.

Re claim 22: Willey teaches a system for secure transfer of multimedia content comprising a first communication device in communication with a second communication device, the first communication device comprising:

processing means for (¶34):

sharing the common secret with the second communication device if the second communication device is compliant (¶56-¶58; *after the exchanged digits are validated, the key agreement proceeds*); and determining a distance measurement between the first and second devices, said distance measurement comprising (Fig 11, elts 200 & 1010; Fig 11a, elts 46 & 48; ¶71; ¶76):

transmitting a spread-spectrum first signal from the first device to the second device at a first time (¶12; Fig 11a, 40; ¶76);

determining the distance based on the difference between the first time and the second time device (Fig 11, elts 200 & 1010; Fig 11a, elts 46 & 48; ¶71; ¶76); and

using the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the multimedia data is transmitted from the first communication device to the second communication device (Fig 11a, elts 48 & 50); and

the second communication device comprising means for playing back the multimedia content (¶8; ¶34; ¶55).

While Willey teaches receiving the first signal modified by the common secret at a second time (Fig 11a, elts 42 & 44; ¶76). Willey does not expressly disclose said modification being associated with modification of spreading codes of the spread spectrum first signal.

Yet, Rofheart teaches said modification being associated with modification of spreading codes of the spread spectrum first signal (¶67; ¶97; ¶159-¶160).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey with the spread-spectrum communication signals of Rofheart, for the purpose of providing secured communication between two parties wherein the secured communication is resistant from jamming; spread-spectrum signals have the known utility of providing secure communication resistant to natural interference and jamming.

It is further held that it would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute the asymmetric cipher of Rofheart with the symmetric cipher of Willey as symmetric ciphers are faster and not computer process intensive.

The combination of Willey and Rofheart does not expressly disclose performing an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device.

Overy teaches performing an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device (Fig 4, elts 35 & 36; ¶8-¶9; ¶40).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey and Rofheart with the teachings of Overy, for the purpose of uniquely identifying devices and preventing unauthorized or unknown devices from joining a protected network.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 14-19 and 21 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 3, 5-8 and 11 of copending Application No. 10/521858. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following:

Re instant claim 14:

Instant claim 14	Copending claim 6 (which encompasses the limitations of independent claim 1)
A method of determining whether multimedia data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of: performing a distance measurement between the first communication device and the second communication device, wherein the first and the second communication device share a common secret which has been shared before performing the distance measurement	A method for a first communication device to performing authenticated distance measurement between said first communication device and a second communication device, wherein the first and the second communication device share a common secret and wherein the authenticated distance measurement comprises …
performing an authentication check on the second communication device, by checking whether the second	performing an authentication check from the first communication device on the second communication device, by

communication device is compliant with a set of predefined compliance rules;	checking whether said second communication device is compliant with a set of a predefined compliance rules;
sharing the common secret with the second communication device if the second communication device is compliant; and	if the second communication device is compliant, sharing said common secret by transmitting said secret to the second communication device,
using the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel.	wherein the common secret has been shared before performing the distance measurement.

The first and second communication devices are synonymous with one-another between the instant and copending claim; this is further held in the distance measurement, common secret and compliance rules.

However, the copending claim does not expressly disclose the common secret being used to modify the spreading code of a spread-spectrum communication signal between the first device and the second device, and transmitting multimedia data from the first communication device to the second communication device over the secure authenticated channel.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of the instant claim with the teachings of the copending claim, for the purpose of providing a communications service amongst devices that have mutually authenticated one another; mutual authentication is well known in the art prior to engaging in some form of communication in order to identify and protect both parties. Using spreading code of a spread-spectrum communication signal is for the purpose of providing secured communication between two parties wherein the secured communication is resistant from jamming; spread-spectrum signals have the known utility of providing secure communication resistant to natural interference and jamming.

Re instant claim 15: Instant claim 15 is rejected as similar in scope to claim 6; the rationale is applied *supra*.

Re instant claim 17: Instant claim 17 is rejected as similar in scope to claim 6.

Re instant claim 18: Instant claim 18 is rejected as similar in scope to claim 5.

Re instant claim 19: Instant claim 19 is rejected as similar in scope to claim 7.

Re instant claim 21: Instant claim 21 is rejected under provisional obviousness-double patenting as it pertains to copending claims 1, 6 & 11.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim 20 provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 6 of copending Application No. 10/521858 in view of Willey (U.S. Pat App Pub 2003/0065918 A1).

Re instant claim 20: Instant claim 14 with respect to copending claim 6 has been addressed supra. However, Willey teaches the step of sharing said common secret comprises executing one of a key transport protocol and a key agreement protocol (Fig 5a, elts 3, 4, 5 & 7; ¶40).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of copending claim 6 with the teachings of Willey, for the purpose of securely negotiating a key between two communication devices; Diffie-Hellman is known in the art as secure key agreement protocol.

This is a provisional obviousness-type double patenting rejection.

Claim 22 provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 6 of copending Application No. 10/521858 in view of Overy et al (U.S. Pat App Pub 2003/0220765 A1), hereinafter referred to as Overy.

Re instant claim 22: Instant claim 22 with respect to copending claim 6 has been addressed supra.

However, the copending claim does not expressly disclose the common secret being used to modify the spreading code of a spread-spectrum communication signal between the first device and the second device, and transmitting multimedia data from the first communication device to the second communication device over the secure authenticated channel.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of the instant claim with the teachings of the copending claim, for the purpose of providing a communications service amongst devices that have mutually authenticated one another; mutual authentication is well known in the art prior to engaging in some form of communication in order to identify and protect both parties. Using spreading code of a spread-spectrum communication signal is for the purpose of providing secured communication between two parties wherein the secured communication is resistant from jamming; spread-spectrum signals have the known utility of providing secure communication resistant to natural interference and jamming.

However, copending claim 6 does not expressly disclose performing an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device.

Overy teaches performing an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device (Fig 4, elts 35 & 36; ¶8-¶9; ¶40).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of the instant claim with the teachings of Overy, for the purpose of uniquely identifying devices and preventing unauthorized or unknown devices from joining a protected network.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Darren B. Schwartz whose telephone number is (571)270-3850. The examiner can normally be reached on 7am-5pm EST, Monday-Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. B. S./
Examiner, Art Unit 2435

/HOSUK SONG/
Primary Examiner, Art Unit 2435

28

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	Kamperman, F.	Attn. No.: 2002P02007US (formerly NL020681US2)
SERIAL NO.:	12/508,917	EXAMINER: Schwartz, D.B.
FILED:	July 24, 2009	ART UNIT: 2435
		CONFIRMATION No.: 8927

FOR: ***SECURE AUTHENTICATED DISTANCE MEASUREMENT***

Mail Stop: RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE FOR CONTINUED EXAMINATION
and
PRELIMINARY AMENDMENT

Dear Sir:

In response to the Final Office Action dated February 17, 2011, and the Advisory Action, dated May 5, 2011, the Applicant hereby timely submits this paper within two (2) months (until **July 18, 2011**) of the mailing date of a Notice of Appeal filed on May 17, 2011 (July 17, 2011 being a Sunday), and requests amendment of the above-identified application as follows wherein:

Amendments made to the Claims begin on page 2, and

Remarks begin on page 6.

IN THE CLAIMS:

Kindly replace the claims of record with the following full set of claims:

1 – 13 (Cancelled)

14. (Currently amended) A method of determining whether multimedia data stored on a first communication device (201, 301) are to be accessed by a second communication device (203, 303), the method comprising the step of:

performing (209) a distance measurement between the first communication device and the second communication device, wherein the first and the second communication device share a common secret which has been shared before performing the distance measurement~~, the common secret being used to modify the spreading code of a spread-spectrum communication signal between the first device and the second device,~~ the method further comprising the steps of:

performing (205) an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with a set of predefined compliance rules;

securely sharing (207) the common secret with the second communication device if the second communication device is compliant, wherein the common secret is used to modify only the spreading code of a spread-spectrum communication signal between the first device and the second device; and

using (211) the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the multimedia data is transmitted from the first communication device to the second communication device.

15. (Previously presented) The method according to claim 14, wherein the authenticated distance measurement further comprises the steps of:

transmitting (309) a first signal from the first communication device (201, 301) to the second communication device at a first time t1, the second communication device being adapted (311) for receiving the first signal;

generating (313) a second signal by modifying the received first signal according to the common secret and transmitting (315) the second signal to the first device;

receiving (317) the second signal at a second time t2;

checking (319) if the second signal has been modified according to the common secret; and

determining (323) the distance between the first and the second communication device according to a time difference between t1 and t2.

16. (Cancelled)

17. (Previously presented) The method according to claim 15, wherein the step of checking (319) if the second signal has been modified according to the common secret comprises the steps of:

generating a third signal by modifying the first signal according to the common secret; and

comparing the third signal with the received second signal.

18. (Previously presented) The method according to claim 15, wherein the first signal and the common secret are bit words and where the second signal comprises information being generated by performing an XOR between the bit words.

19. (Previously presented) The method according to claim 14, wherein the authentication check (205) further comprises the step of checking if the identification of the second device is compliant with an expected identification.

20. (Previously presented) The method according to claim 14, in which the step of sharing (207) said common secret comprises executing one of a key transport protocol and a key agreement protocol.

21. (Currently amended) A first communication device (201, 301, 406) configured for determining whether multimedia data stored on the first communication device are to be accessed by a second communication device (203, 303), the device comprising:

means for performing distance measurement between the first communication device and the second communication device, wherein the first communication device comprises a memory storing a common secret, which is securely transmitted to and also stored on the second communication device, ~~which~~ said secret being ~~is~~ used to modify only a spreading code of a spread-spectrum communication signal between the first device and the second device, the first communication device being configured (403, 411, 413, 417) for sharing the common secret before performing the distance measurement, wherein the first communication device further comprises means for:

performing (205) an authentication check of the second communication device, by checking whether the second communication device is compliant with a set of predefined compliance rules;

sharing (207) the common secret with the second communication device if the second communication device is compliant; and

using (211) the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel and transmitting multimedia data from the first communication device to the second communication device over the secure authenticated channel.

22. (Currently amended) A system for secure transfer of multimedia content comprising a first communication device (201, 301, 406) in communication with a second communication device (203, 303), the first communication device comprising:

processing means for:

performing (205) an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device;

securely sharing (207) [[the]] a common secret with the second communication device if the second communication device is compliant; and

determining a distance measurement between the first and second devices, said distance measurement comprising:

transmitting a spread-spectrum first signal from the first device to the second device at a first time;

receiving the first signal modified by the common secret at a second time, said modification being associated with modification of only spreading codes of the spread spectrum first signal; and

determining the distance based on the difference between the first time and the second time; and

using (211) the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the multimedia data is transmitted from the first communication device to the second communication device; and

the second communication device comprising means for playing back the multimedia content.

REMARKS

Entry of this Amendment and reconsideration are respectfully requested in view of the amendments made to the claims and for the remarks made herein.

Claims 14, 15 and 17-22 are pending and stand rejected.

Claims 14, 21 and 22 are independent claims.

Claims 14, 21 and 22 have been amended.

Claims 14 and 20-21 stand rejected under 35 USC 103(a) as being unpatentable over Willey (US 2003/0065918) in view of Rofheart (US 2005/0265503). Claims 15, 16 and 18 stand rejected under 35 USC 103(a) as being unpatentable over Willey in view of Rofheart and further in view of Lundkvist (US 2003/0184431). Claim 17 stands rejected under 35 USC 103(a) as being unpatentable over Willey in view of Rofheart and Lundkvist and further in view of Caputo (USP 5,778,071). Claim 19 stands rejected under 35 USC 103(a) as being unpatentable over Willey in view of Rofheart and Simon (USP 5,937,065). Claim 22 stands rejected under 35 USC 103(a) as being unpatentable over Wiley and Rofheart and further in view of Overy (2003/0220765).

Claims 14-19 and 21 stand provisionally rejected on the ground of nonstatutory obviousness-type double patenting over co-pending application 10/521,858. Claim 20 stands provisionally rejected on the ground of nonstatutory obviousness-type double patenting over co-pending application 10/521,858 in view of Willey. Claim 22 stands provisionally rejected on the ground of nonstatutory obviousness-type double patenting over claim 6 of co-pending application 10/521,858 in view of Overy.

With regard to the rejection of the claims, Applicant repeats the remarks made in Applicant's Response to the Final Office Action issued in this matter, as if in full herein.

However, in order to advance the prosecution of this matter, in view of the remarks made in the Advisory Action, Applicant has amended the independent claims to more clearly recite that the first device ***securely*** transmits the common secret key to the second device. No new matter has been added. Support for the amendment may be found at least on page 7, lines 2-5; "Then in 207, the first device 201 exchanges a secret with the second device 203, which e.g. could be performed by transmitting a random generated bit word to 203. ***The secret should be shared securely,*** e.g. according to some key management protocol as described in e.g. ISO 11770.") See also, page 11, lines 11-2; "if the second communication device is compliant, s***haring said common secret by transmitting said secret to the second communication device***."

In the reply provided in the Advisory Action, the Examiner refers to Willey disclosing a D-H (Diffie-Hellman) algorithm for determining a common secret key that may be used by the two devices. The Examiner further states that it would be obvious to incorporate the pairing of Willey with the public key of Rofheart.

However, in a D-H algorithm, each device selects a random number to be used in a common value determination process and provides this number to the other device. The other device then, individually, determines a common value using the provided number.

For example, device 1 may select an initial value of 6 and device two may select an initial value of 9. The two devices may have knowledge of modulus values 7 and 11, which are used in the common valued determination process.

Device one ma determine a value 4 from 7^6(mod 11), which is transmitted to device 2. Similarly device 2 generates a value 8 from 7^9(mod 11), which is transmitted to device 1. Each determined value is transmitted to the other device in an un-encoded manner (i.e., not secure).

Device 1, using the received value 8, determines a common value 3 from 8^6 (mod 11) and device 2, using the receive value 4, determines the common value 3 from 4^9 (mod 11).

Thus, both device 1 and device 2 have knowledge of a value that may be used in encrypting messages thereafter.

However, although D-H may be used to determine a common value that may be used to encode further transmission, each device has independently generated a common value.

Hence, there is no need for device 1 to securely share the common value with the second device.

In addition, even if it could be assumed that the value that device 1 transmits to device 2 (i.e., value 4, in this exemplary case) is comparable to the common secret value, the value is transmitted in the clear and is not securely transmitted, as is recited in the claims.

According, the use of the D-H algorithm disclosed by Willey fails to disclose the elements recited in the claims.

Hence, even though the Advisory Action asserts that the pairing described by Willey (with regard to D-H algorithm) may be used to determine a common secret key, the use of the D-H algorithm fails to disclose the element of "***<u>sharing (207) the common secret with the second communication device</u>*** if the second communication device is compliant".

In addition, Rofheart discloses a public/private key exchange, where device 1 provides a public key, in the clear. Hence, Rofheart also fails to disclose the use of a secure communication to ***share the common secret key***.

Hence, neither Willey nor Rofheart teaches or discloses sharing the common secret key, and assuming the use of a D-H algorithm as taught by Willey, there is no motivation to share the common secret key, as recited in the clams, the combination of the references cannot render unpatentable the subject matter recited in the independent claims.

In addition, neither Willey nor Rofheart discloses that the spread spectrum codes are modified by the common secret key.

The Advisory Action states that Rofheart (69, 97, 159-160 teaches "the use of a spread –spectrum signals to communication between devices and transmitting encrypted messages between the devices," however, the Applicant again submits that neither Rofheart nor Willey provide any teaching that the spread-spectrum codes are encrypted. Rather Rofheart discloses the message being encrypted and not the codes.

However, to more clearly recite the invention claimed, the independent claims have been amended to further recite that only the spectrum codes are encrypted. No new matter has been added. Support for the amendment may be found at least on page 7, lines 18-21; "In a specific example a direct sequence spread spectrum signal is used for distance measurement; this signal could be modified by XORing the chips (e.g. spreading code consisting of 127 chips) of the direct sequence code by the bits of the secret (e.g. secret consists also of 127 bits). Also, other mathematical operations as XOR could be used."

In determining whether a claim is obvious in view of the teachings found prior to the filing of the instant application, the Court in *KSR v. Teleflex* (citation omitted) held that a bright light application of the teaching, suggestion and motivation test (TSM) may be used as a helpful hint in determining obviousness and that the factors for determining obviousness enumerated in *Graham v. John Deere* (i.e., the scope and content of the prior art, the level of ordinary skill in the art, the differences between the claimed invention and the prior art and objective indicia of non-obviousness) are to be applied.

The teaching, suggestion and motivation test held that a claimed invention is prima facie obvious when three basic criteria are met. First, there must be some suggestion or motivation, either in the reference themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the teachings therein. Second, there must be a reasonable expectation of success. And, third, the prior art reference or combined references must teach or suggest all the claim limitations.

For the amendments made to the claims and for the remarks made herein, Applicant submits that claims, 14, 21 and 22, and the claims dependent therefrom, are not rendered unpatentable over the cited references.

With regard to the rejection of the remaining claims under 35 USC 103 (a), Applicant submits that these claims depend from respective ones of the independent claims and inherit the subject matter claimed therein; such subject matter is patently distinguishable over the teachings of Willey and Rofheart. None of the other cited references provide any teaching regarding a common secret key used to securely share the secret key or to modify the spreading codes of a spread spectrum system using the secret key.

Accordingly, the remaining claims are also not rendered unpatentable by the cited references by virtue of their dependency upon an allowable base claim.

With regard to the rejection of the claims as being unpatentable under the judicially-created doctrine of double patenting, Applicant repeats the comments made in the prior response, as if in full herein.

However, Applicant respectfully requests that the rejection be held in abeyance until either the instant application or the cited application issues and the claims may be compared to determine whether the rejection is still applicable.

For the arguments presented, herein, applicant submits that the rejections of the claims have been overcome and respectfully requests that the rejections be withdrawn and that a Notice of Allowance be issued.

Applicant denies any statement, position or averment stated in the Office Action that is not specifically addressed by the foregoing. Any rejection and/or points of argument not addressed are moot in view of the presented arguments and no arguments are waived and none of the statements and/or assertions made in the Office Action is conceded.

Applicant makes no statement regarding the patentability of the subject matter recited in the claims prior to this Amendment and has amended the claims solely to facilitate expeditious prosecution of this patent application. Applicant respectfully reserves the right to pursue claims, including the subject matter encompassed by the originally filed claims, as presented prior to this Amendment, and any additional claims in one or more continuing applications during the pendency of the instant application.

In order to advance the prosecution of the matter, applicant respectively requests that any errors in form that do not alter the substantive nature of the arguments presented herein be transmitted telephonically to the applicant's representative so that such errors may be quickly resolved or pursuant to MPEP 714.03 be entered into the record to avoid continued delay of the prosecution of this matter any further.

MPEP 714.03 affords the Examiner the discretion, pursuant to 37 CFR 1.135 (c), to enter into the record a bona fide attempt to advance the application that includes minor errors in form.

"[a]n Examiner may treat an amendment not fully responsive to a non-final Office Action by: (A) accepting the amendment as an adequate reply to the non-final Office action to avoid abandonment ... (B) notifying the applicant that the reply must be completed... (C) setting a new time period for applicant to complete the reply ...

The treatment to be given to the amendment depends upon:

(A) whether the amendment is bona fide; (B) whether there is sufficient time for applicant's reply ... (C) the nature of the deficiency.

Where an amendment substantially responds to the rejections, objections or requirements in a non-final Office action (and is bona fide attempt to advance the application to final action) but contains a minor deficiency (e.g., fails to treat every rejection, objection or requirement), the examiner may simply act on the amendment and issue a new (non-final or final) Office action. The new Office action may simply reiterate the rejection, objection or requirement not addressed by the amendment (or otherwise indicate that such rejection, objection or requirement is no longer applicable).

This course of action would not be appropriate in instances in which an amendment contains a serious deficiency (e.g., the amendment is unsigned or does not appear to have been filed in reply to the non-final Office action)..."

However, if the Examiner believes that such minor errors in form cannot be entered into the record or that the disposition of any issues arising from this response may be best resolved by a telephone call, then the Examiner is invited to contact applicant's representative at the telephone number listed below to resolve such minor errors or issues.

No fees are believed necessary for the timely filing of this paper.

Respectfully submitted,

Date: July 17, 2011

/Carl A. Giordano/

By: Carl A. Giordano
Attorney for Applicant
Registration No. 41,780
(914) 391 8104)

Mail all correspondence to:
Michael E. Belk, Esq.
US PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9643
Fax: (914) 332-0615

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being:
[ ] Transmitted electronic by the currently available EFS system;
[ ] Transmitted by facsimile to 571 273 8300;
[ ] Placed with the US Postal Service with First Class postage attached to the address indicated above;
on July ________, 2011

________________________	________________________
Print Name	Signature

29

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	Kamperman, F.	Attn. No.: 2002P02007US
SERIAL NO.:	12/508,917	EXAMINER: Schwartz, D.B.
FILED:	July 24, 2009	ART UNIT: 2435
		CONFIRMATION No.: 8927

FOR: ***SECURE AUTHENTICATED DISTANCE MEASUREMENT***

Mail Stop: Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

Dear Sir:

In response to the Office Action dated September 14, 2011, the Applicant hereby timely submits this paper within three (3) months (until **December 14, 2011**) of the mailing date of the Office Action and requests amendment of the above-identified application as follows wherein:

Amendments made to the Claims begin on page 2, and

Remarks begin on page 6.

IN THE CLAIMS:

Kindly replace the claims of record with the following full set of claims:

1 – 13 (Cancelled)

14. (Currently amended) A method of determining whether multimedia data stored on a first communication device (201, 301) are to be accessed by a second communication device (203, 303), the method comprising the step of:

performing (209) a distance measurement between the first communication device and the second communication device, wherein the first and the second communication device share a common secret which has been shared before performing the distance measurement, the method further comprising the steps of:

performing (205) an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with a set of predefined compliance rules;

securely sharing (207) the common secret with the second communication device if the second communication device is compliant, wherein the common secret is used to modify only ~~the~~ a spreading code of a spread-spectrum communication signal between the first device and the second device; and

using (211) the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the multimedia data is transmitted from the first communication device to the second communication device.

15. (Previously presented) The method according to claim 14, wherein the authenticated distance measurement further comprises the steps of:

transmitting (309) a first signal from the first communication device (201, 301) to the second communication device at a first time t1, the second communication device being adapted (311) for receiving the first signal;

generating (313) a second signal by modifying the received first signal according to the common secret and transmitting (315) the second signal to the first device;

receiving (317) the second signal at a second time t2;

checking (319) if the second signal has been modified according to the common secret; and

determining (323) the distance between the first and the second communication device according to a time difference between t1 and t2.

16. (Cancelled)

17. (Previously presented) The method according to claim 15, wherein the step of checking (319) if the second signal has been modified according to the common secret comprises the steps of:

generating a third signal by modifying the first signal according to the common secret; and

comparing the third signal with the received second signal.

18. (Previously presented) The method according to claim 15, wherein the first signal and the common secret are bit words and where the second signal comprises information being generated by performing an XOR between the bit words.

19. (Previously presented) The method according to claim 14, wherein the authentication check (205) further comprises the step of checking if the identification of the second device is compliant with an expected identification.

20. (Previously presented) The method according to claim 14, in which the step of sharing (207) said common secret comprises executing one of a key transport protocol and a key agreement protocol.

21. (Previously presented) A first communication device (201, 301, 406) configured for determining whether multimedia data stored on the first communication device are to be accessed by a second communication device (203, 303), the device comprising:

means for performing distance measurement between the first communication device and the second communication device, wherein the first communication device comprises a memory storing a common secret, which is securely transmitted to and also stored on the second communication device, said secret being ~~is~~ used to modify only a spreading code of a spread-spectrum communication signal between the first device and the second device, the first communication device being configured (403, 411, 413, 417) for sharing the common secret before performing the distance measurement, wherein the first communication device further comprises means for:

performing (205) an authentication check of the second communication device, by checking whether the second communication device is compliant with a set of predefined compliance rules;

sharing (207) the common secret with the second communication device if the second communication device is compliant; and

using (211) the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel and transmitting multimedia data from the first communication device to the second communication device over the secure authenticated channel.

22. (Previously presented A system for secure transfer of multimedia content comprising a first communication device (201, 301, 406) in communication with a second communication device (203, 303), the first communication device comprising:

processing means for:

performing (205) an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device;

securely sharing (207) a common secret with the second communication device if the second communication device is compliant; and

determining a distance measurement between the first and second devices, said distance measurement comprising:

transmitting a spread-spectrum first signal from the first device to the second device at a first time;

receiving the first signal modified by the common secret at a second time, said modification being associated with modification of only spreading codes of the spread spectrum first signal; and

determining the distance based on the difference between the first time and the second time; and

using (211) the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the multimedia data is transmitted from the first communication device to the second communication device; and

the second communication device comprising means for playing back the multimedia content.

REMARKS

Entry of this Amendment and reconsideration are respectfully requested in view of the amendments made to the claims and for the remarks made herein.

Claims 14, 15 and 17-22 are pending and stand rejected.

Claims 14, 21 and 22 are independent claims.

Claim 14 has been amended.

Claim 14 is objected to. Claims 14 and 20-21 stand rejected under 35 USC 103(a) as being unpatentable over Willey (US 2003/0065918) in view of Rodman(US 2003/0112978). Claims 15 and 18 stand rejected under 35 USC 103(a) as being unpatentable over Willey in view of Rodman and further in view of Lundkvist (US 2003/0184431). Claim 17 stands rejected under 35 USC 103(a) as being unpatentable over Willey in view of Rodman and Lundkvist and further in view of Caputo (USP 5,778,071). Claim 19 stands rejected under 35 USC 103(a) as being unpatentable over Willey in view of Rodman and Simon (USP 5,937,065). Claim 22 stands rejected under 35 USC 103(a) as being unpatentable over Wiley and Rodman and further in view of Overy (2003/0220765).

Claims 14-19 and 21 stand provisionally rejected on the ground of nonstatutory obviousness-type double patenting over claims 1, 5-8 and 11 of co-pending application no. 10/521,858 in view of Rodman. Claim 20 stands provisionally rejected on the ground of nonstatutory obviousness-type double patenting over co-pending application 10/521,858 in view of Rodman. Claim 22 stands provisionally rejected on the ground of nonstatutory obviousness-type double patenting over claim 6 of co-pending application 10/521,858 in view of Rodman [Overy].

With regard to the objection to claim 1, Applicant thanks the Examiner for his observation and has amended claim 1 to correct the error noted.

Applicant submits that the reason for the objection has been overcome.

With regard to the rejection of the claims as being unpatentable over the combination of Willey and Rodman, Applicant respectfully disagrees with and explicitly traverses the rejection of the claims.

In supporting the rejection of the claims, the Office Action refers to Willey for teaching a method of determining whether multimedia data stored on a first communication device are to be accessed by a second communication device; performing a distance measurement… wherein the first and second communication device share a common secret which has been shared before performing the distance measurement, the method further comprising the steps performing an authentication check by checking whether the second device is compliant with a set of predefined compliance rules, securely sharing the common secret with the second communication device, and using the common secret over which the multimedia data is transmitted.

The Office action acknowledges that Willey does not expressly disclose, yet Rodman teaches the common secret is used to modify only the spreading code of a spread-spectrum (para19, para 21-23).

Applicant respectfully disagrees with and repeats the remarks made in Applicant's Response to the Final Office Action of February 12, 2011 and the Advisory Action of May 5, 2011, as if in full herein, with regard to the Willey reference.

In particular, Willey discloses a Diffie-Hellman (D-H) algorithm that provides for each device to determine a secret code based on publically distributed values. From the publically distributed values used in conjunction with a known algorithm, a secure code may be developed by each device that may be used for subsequent encryption of messages (using the developed secret code) among the devices.

However, although a D-H algorithm may be used to determine a common value that may be used to encode further transmission, each device independently generates a common value.

Hence, there is no need for device 1 to s***ecurely share*** the common value with the second device.

Hence, Willey fails to disclose the element of "***securely sharing (207) the common secret with the second communication device*** **if the second communication device is compliant"**. Willey fails to disclose securely transmitting the common secret. Rather Willey teaches publically transmitting data that may be used to determine a common secret.

With regard to teaching of Rodman, Rodman teaches a system wherein an encryption key is transmitted from one device to other devices using an audio signal to prevent the intercept of the encryption key by non-authorized devices. The transmitting device of Rodman encodes the encryption key as an acoustic signal and transmits the acoustic signal with a low volume to prevent the signal being distributed outside a desired area and to limit the inconvenience of the acoustic signal on other parties within the desired area (see step 306, figure 3). The receiving systems within the desired area (having the appropriated decoding equipment) receiving the acoustic signal decode the received signal to obtain the transmitted encryption key (step 308, figure 3).

The encryption key is then used to encrypt messages between the devices within the desired area (step 314, figure 3).

Rodman, thus, teaches a system wherein an encryption key is transmitted in as an audio signal to transmit the encryption key among devices within a desired area. However, Rodman teaches that the encryption key, after being decoded by devices that have the appropriate decoding equipment, is used to encrypt and transmit messages among the devices.

Rodman fails to disclose that the encryption key is used only to encrypt the spreading codes (i.e., "wherein the common secret is used to ***modify only a***

spreading code of a spread-spectrum communication signal between the first device and the second device").

That is, while Rodman teaches sending encryption keys using an audio signal, the decoded encryption key is used to encrypt messages and then the encrypted messages may then be encoded using a spread-spectrum protocol (i.e., the encrypted messages are encoded with the spreading code of the spread-spectrum protocol).

Nowhere does Rodman teach that only the spreading codes are encrypted with the encryption key, as is recited in the claims.

Neither Willey nor Rodman discloses that the spread codes of the spread spectrum signal are encrypted by the common secret key.

In determining whether a claim is obvious in view of the teachings found prior to the filing of the instant application, the Court in *KSR v. Teleflex* (citation omitted) held that a bright light application of the teaching, suggestion and motivation test (TSM) may be used as a helpful hint in determining obviousness and that the factors for determining obviousness enumerated in *Graham v. John Deere* (i.e., the scope and content of the prior art, the level of ordinary skill in the art, the differences between the claimed invention and the prior art and objective indicia of non-obviousness) are to be applied.

The teaching, suggestion and motivation test held that a claimed invention is prima facie obvious when three basic criteria are met. First, there must be some suggestion or motivation, either in the reference themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the teachings therein. Second, there must be a reasonable expectation of success. And, third, the prior art reference or combined references must teach or suggest all the claim limitations.

In this case, Applicant submits that claims, 14, 21 and 22, and the claims dependent therefrom, are not rendered unpatentable over the cited references.

Neither of the cited references provides any teaching regarding modifying only the spreading codes of a spread spectrum system using the common secret key.

With regard to the rejection of the remaining claims under 35 USC 103 (a), Applicant submits that these claims depend from respective ones of the independent claims and inherit the subject matter claimed therein; such subject matter being patently distinguishable over the teachings of Willey and Rodman.

None of the other cited references provides any teaching that would correct the deficiency found to exist in the teachings of Willey and Rodman.

Accordingly, the remaining claims are also not rendered unpatentable by the cited references by virtue of their dependency upon an allowable base claim.

With regard to the rejection of the claims as being unpatentable under the judicially-created doctrine of double patenting, Applicant again repeats the comments made in the prior response, as if in full herein.

Applicant respectfully requests that the rejection be held in abeyance until either the instant application or the cited application issues and the claims may be compared to determine whether the rejection is still applicable.

In addition, claim 1 of the referred to application refers to a method for transmitting signals between two devices wherein a second device transmits a first signal modified by the secret code and the first device receives the modified second signal, modifies the first signal by the secret code and determines whether the locally modified first signal is comparable to the modification made to the first signal made by the second device. However none of the claims dependent from claim 1, that the common secret is shared by a secure transmission. Nor, as shown above, does Rodman discloses that "wherein the common secret is used to modify ***only a spreading code of a spread-spectrum communication signal*** between the first device and the second device."

In fact, the referred-to application fails to disclose any modification of the spreading code of a spread-spectrum communication signal, as is recited in the claims.

Hence, the subject matter recited in the instant application is patently distinguishable from that recited in the referred-to patent application, as the referred-to patent application fails to disclose modification of the spreading codes, as is recited in the claims.

For the arguments presented, herein, applicant submits that the rejections of the claims have been overcome and respectfully requests that the rejections be withdrawn and that a Notice of Allowance be issued.

Applicant denies any statement, position or averment stated in the Office Action that is not specifically addressed by the foregoing. Any rejection and/or points of argument not addressed are moot in view of the presented arguments and no arguments are waived and none of the statements and/or assertions made in the Office Action is conceded.

Applicant makes no statement regarding the patentability of the subject matter recited in the claims prior to this Amendment and has amended the claims solely to facilitate expeditious prosecution of this patent application. Applicant respectfully reserves the right to pursue claims, including the subject matter encompassed by the originally filed claims, as presented prior to this Amendment, and any additional claims in one or more continuing applications during the pendency of the instant application.

In order to advance the prosecution of the matter, applicant respectively requests that any errors in form that do not alter the substantive nature of the arguments presented herein be transmitted telephonically to the applicant's representative so that such errors may be quickly resolved or pursuant to MPEP 714.03 be entered into the record to avoid continued delay of the prosecution of this matter any further.

MPEP 714.03 affords the Examiner the discretion, pursuant to 37 CFR 1.135 (c), to enter into the record a bona fide attempt to advance the application that includes minor errors in form.

"[a]n Examiner may treat an amendment not fully responsive to a non-final Office Action by: (A) accepting the amendment as an adequate reply to the non-final Office action to avoid abandonment … (B) notifying the applicant that the reply must be completed… (C) setting a new time period for applicant to complete the reply …

The treatment to be given to the amendment depends upon:

(A) whether the amendment is bona fide; (B) whether there is sufficient time for applicant's reply … (C) the nature of the deficiency.

Where an amendment substantially responds to the rejections, objections or requirements in a non-final Office action (and is bona fide attempt to advance the application to final action) but contains a minor deficiency (e.g., fails to treat every rejection, objection or requirement), the examiner may simply act on the amendment and issue a new (non-final or final) Office action. The new Office action may simply reiterate the rejection, objection or requirement not addressed by the amendment (or otherwise indicate that such rejection, objection or requirement is no longer applicable).

This course of action would not be appropriate in instances in which an amendment contains a serious deficiency (e.g., the amendment is unsigned or does not appear to have been filed in reply to the non-final Office action)…"

However, if the Examiner believes that such minor errors in form cannot be entered into the record or that the disposition of any issues arising from this response may be best resolved by a telephone call, then the Examiner is invited to contact applicant's representative at the telephone number listed below to resolve such minor errors or issues.

No fees are believed necessary for the timely filing of this paper.

Respectfully submitted,

Date: December 2, 2011

/Carl A. Giordano/

By: Carl A. Giordano
Attorney for Applicant
Registration No. 41,780
(914) 391 8104)

Mail all correspondence to:
Michael E. Belk, Esq.
US PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9643
Fax: (914) 332-0615

CERTIFICATE OF MAILING UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being:
[ ] Transmitted electronic by the currently available EFS system;
[ ] Transmitted by facsimile to 571 273 8300;
[ ] Placed with the US Postal Service with First Class postage attached to the address indicated above;
on December________, 2011

________________________ Print Name

________________________ Signature

30

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/508,917	07/24/2009	Franciscus Lucas Antonius Johannes KAMPERMAN	2002P02007 US	8927

24737 7590 01/05/2012
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SCHWARTZ, DARREN B	
ART UNIT	**PAPER NUMBER**
2435	
NOTIFICATION DATE	**DELIVERY MODE**
01/05/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

vera.kublanov@philips.com
debbie.henn@philips.com
marianne.fox@philips.com

Office Action Summary	Application No. 12/508,917	Applicant(s) KAMPERMAN, FRANCISCUS LUCAS ANTONIUS JO
	Examiner DARREN B. SCHWARTZ	Art Unit 2435

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2011*.

2a)□ This action is **FINAL**. 2b)□ This action is non-final.

3)□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *14,15 and 17-22* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)□ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *14,15 and 17-22* is/are rejected.

8)□ Claim(s) _____ is/are objected to.

9)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)□ The specification is objected to by the Examiner.

11)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

In a response filed 14 December 2011, Applicant amends claim 14.

Claims 14, 15 and 17-22 are presented for examination.

Response to Arguments

1. In light of Applicant's amendment to claim 14 the claim objection is withdrawn.

Applicant's arguments filed 14 December 2011 have been fully considered but they are not persuasive.

2. On page 7 of Remarks, Applicant states: "Applicant respectfully disagrees with and repeats the remarks made in Applicant's Response to the Final Office Action of February 12, 2011 and the Advisory Action of May 5, 2011, as if in full herein, with regard to the Willey reference."

The Examiner notes that such arguments presented by Applicant were associated with corresponding rebuttals set forth by the Examiner. Merely incorporating arguments "as if in full herein" and "repeat[ing] the remarks" does not address the entirety of the Examiner's position. Merely repeating an argument without consideration of the Examiner's response fails to address the entirety of the Examiner's position; accordingly, only arguments presented in the instant response filed 14 December 2011 are considered.

3. On pages 7 and 8 of remarks, Applicant argues: “In particular, Willey discloses a Diffie-Hellman (D-H) algorithm that provides for each device to determine a secret code based on publically distributed values. From the publically distributed values used in conjunction with a known algorithm, a secure code may be developed by each device that may be used for subsequent encryption of messages (using the developed secret code) among the devices. However, although a D-H algorithm may be used to determine a common value that may be used to encode further transmission, each device independently generates a common value. Hence, there is no need for device 1 to securely share the common value with the second device. Hence, Willey fails to disclose the element of ‘securely sharing (207) the common secret with the second communication device if the second communication device is compliant’. Willey fails to disclose securely transmitting the common secret. Rather Willey teaches publically transmitting data that may be used to determine a common secret.”

The Examiner notes the following has been held: “All of the disclosures in a reference must be evaluated for what they fairly teach one of ordinary skill in the art.” *In re Lemelson*, 397 F.2d 1006, 1009 (CCPA 1968). “The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain.” (quoting *In re Boe*, 355 F.2d 961, 965 (CCPA 1966)).

Willey explicitly states:

> “If the user 400 does not give positive confirmation on both devices 100 and 300 or if the user 400 indicates a mismatch between digits, the pairing can be

> aborted, or it can be restarted with a new key agreement. After the user 400 has given positive confirmation on both the headset 300 and the handset 100, then the devices 100 and 300 are fully authenticated. In the next step 7, the devices 100 and 300 securely establish the link key. For example, the devices 100, 300 can both derive a symmetric encryption key based upon the elliptic curve Diffie-Hellman shared secret. A link key is created, and encrypted using the encryption key and send to the other device 300 which decrypts and stores it. The link key is then be used by the devices 100 and 300 for BLUETOOTH authentication and encryption. Alternately, a long PIN may be sent from one device 100 to the other encrypted with the encryption key. The other device 300 would then decrypt it and then the devices 100 and 300 would establish a link key based upon a shared PIN using the well-known BLUETOOTH procedure." (¶48 with emphasis added by Examiner).

The Examiner applies, *at least*, the highlighted portions of Willey, ¶48, as teaching securely sharing the common secret with the second communication device. The Diffie-Hellman algorithm of Willey is not applied; however, the transmission of the encrypted link key from one device and subsequently received and decrypted by the second device, as taught in ¶48 of Willey, meets the claimed language. The Examiner points out that the advisory action (05 May 2011) addressed this very issue.

4. On page 8 of remarks, Applicant argues: "Rodman, thus, teaches a system wherein an encryption key is transmitted in as an audio signal to transmit the encryption

key among devices within a desired area. However, Rodman teaches that the encryption key, after being decoded by devices that have the appropriate decoding equipment, is used to encrypt and transmit messages among the devices. Rodman fails to disclose that the encryption key is used only to encrypt the spreading codes (i.e. 'wherein the common secret is used to modify only a spreading code of a spreading code of a spread-spectrum communication signal between the first device and the second device'). That is, while Rodman teaches sending encryption keys using an audio signal, the decoded encryption key is used to encrypt messages and then the encrypted messages may then be encoded using a spread-spectrum protocol (i.e., the encrypted messages are encoded with the spreading code of the spread-spectrum protocol). Nowhere does Rodman teach that only the spreading codes are encrypted with the encryption key, as is recited in the claims.

The Examiner disagrees and notes that Applicant's claim recites "wherein the common secret is used to modify only a spreading code of a spreading code of a spreading code of a spread-spectrum communication signal between the first device and the second device" (emphasis added by Examiner). Applicant's argument of "Rodman fails to disclose that the encryption key is used only to encrypt the spreading codes" addressed features not recited in the claim, a.k.a. the claim does not recite "wherein the common secret encrypts only a spreading code …" but states "is used to modify only a spreading code."

Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Willey teaches the spreading code of a spread-spectrum communication signal between a first and second device comprises an encryption key which has been encoded from an n-digit sequence of numbers to a sequence of DTMF tones (¶10) and subsequently decoded (Willey: ¶17-¶19).

In response to the argument that "Nowhere does Rodman teach that only the spreading codes are encrypted with the encryption key, as is recited in the claims," (emphasis added by Examiner), such language is **not** the same as the language recited in the claims; the claims recite "wherein the common secret is used to **modify** only a spreading code of a spread-spectrum communication signal." The language is clearly different and is of different scope; modifying a signal does not imply encryption of a signal, nor does it apply vice-versa. Thus, Applicant's argument is incommensurate with the scope of the claim language. Additionally, although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

5. On page 10 of remarks, Applicant argues: "with regard to the rejection of the claims as being unpatentable under the judicially-created doctrine of double patenting, Applicant again repeats the comments made in the prior response, as if in full herein."

The Examiner notes that such arguments presented by Applicant were associated with corresponding rebuttals set forth by the Examiner. Merely incorporating arguments “as if in full herein" and "repeat[ing] the remarks" does not address the entirety of the Examiner's position. Merely repeating an argument without consideration of the Examiner’s response fails to address the entirety of the Examiner’s position; accordingly, only arguments presented in the instant response filed 14 December 2011 are considered.

6. On page 10 of remarks, Applicant states: “Applicant respectfully requests that the rejection be held in abeyance until either the instant application or the cited application issues and the claims may be compared to determine whether the rejection is still applicable.”

Accordingly, the claims provisionally rejected under the grounds of non-statutory obviousness-type double patenting are sustained.

Applicant continues the statement by arguing on page 10 of Remarks: “Nor as shown above, does Rodman discloses (*sic*) that 'wherein the common secret is used to modify only *a* spreading code of a spread-spectrum communication signal between the first device and the second device."

The Examiner disagrees and refers to the very same rebuttals set forth *supra*.

7. On page 10 of remarks, Applicant argues: "In fact, the referred-to application fails to disclose any modification of the spreading code of a spread-spectrum communication signal, as is recited in the claims."

The Examiner notes that Applicant is not addressing the entirety of the Examiner's position as the Examiner applies copending Application No. 10/521858 in view of "Rodman et al" and not the copending application alone.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 14, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Rodman et al (U.S. Pat App Pub 2003/0112978 A1), hereinafter referred to as Rodman.

Re claim 14: Willey teaches a method of determining whether multimedia data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of

performing a distance measurement between the first communication device and the second communication device (Fig 11, elts 200 & 1010; Fig 11a, elts 46 & 48; ¶71; ¶76), wherein the first and the second communication device share a common secret (Fig 5A; ¶48-¶49) which has been shared before performing the distance measurement (Fig 5A; ¶3; ¶37; ¶48-¶49; Fig 11A, elts 40, 42, 44 & 46), the method further comprising the steps of:

performing an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with a set of predefined compliance rules (¶56-¶58; *instances of values are exchanged and respectively validated between the two devices*);

securely sharing the common secret with the second communication device if the second communication device is compliant (¶48; ¶56-¶58; *after the exchanged digits are validated, a link key is created, and encrypted using the encryption key and sent to the other device where it is decrypted and stored*); and

using the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the multimedia data is transmitted from the first communication device to the second communication device (Fig 11a, elts 48 & 50).

However, Willey does not expressly disclose, yet Rodman teaches the common secret is used to modify only a spreading code of a spread-spectrum (¶17-¶19; ¶21-¶23).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey with the teachings of Rodman, for the purpose of providing secured communication between two parties wherein the secured communication is resistant from jamming; spread-spectrum signals have the known utility of providing secure communication resistant to natural interference and deliberate jamming.

Re claim 20: The combination of Willey and Rodman teaches the step of sharing said common secret comprises executing one of a key transport protocol and a key agreement protocol (Willey: Fig 5A, elts 3, 4, 5 & 7).

Re claim 21: Claim 21 is rejected under similar rationale as those expressed as per claim 14 stated *supra*.

9. Claims 15 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Rodman et al (U.S. Pat App Pub 2003/0112978 A1), hereinafter referred to as Rodman, in further view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist.

Re claim 15: The combination of Willey and Rodman teaches all the limitations of claim 14 as previously stated.

However, Lundkvist teaches:

transmitting a first signal from the first communication device [Fig 1, elt 1] to the second communication device [Fig 1, elt 1] at a first time t1, the second communication device being adapted for receiving the first signal (Fig 2, elts “Message x is determined and X is sent,” –X→, “X is received and decrypted;” ¶32);

generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal to the first device (Fig 2, elts “X is received and decrypted” & "f(x) and is determined and Y1 is sent;" ¶32);

receiving the second signal at a second time t2 (Fig 2, elts: “←Y1—" and "Y1 is received, decrypted, f(x) and T1 are checked;" ¶32);

checking if the second signal has been modified according to the common secret (Fig 2, elt: “Y1 is received, decrypted, f(x) and T1 are checked;" ¶32); and

determining (323) the distance between the first and the second communication device according to a time difference between t1 and t2 (¶11; ¶20; ¶42; ¶53).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey and Rodman with the teachings of Lundkvist, for the purpose of simultaneously validating & authenticating the credentials between two devices and the physical distance between said two devices; while Willey does these events sequentially, Lundkvist provides for these events simultaneously and is thus more efficient.

Re claim 18: The combination of Willey, Rodman and Lundkvist teaches the first signal and the common secret are bit words and where the second signal comprises information being generated by performing an XOR between the bit words (Willey: ¶72-¶73).

10. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, Rodman et al

(U.S. Pat App Pub 2003/0112978 A1), hereinafter referred to as Rodman, and Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, in further view of Caputo et al (U.S. Pat 5778071 A), hereinafter referred to as Caputo.

Re claim 17: The combination of Willey, Rodman and Lundkvist teaches all the limitations of 15 as previously stated.

However, Caputo teaches the step of checking [Fig 5A, elt 64] if the second signal [Fig 5A, elts 66 & 68] has been modified according to the common secret [Fig 5A, elts 62 & 70] comprises the steps of:

generating a third signal [Fig 5A, elts 55 & 62] by modifying the first signal [Fig 5A, elt 54] according to the common secret [Fig 5A, elts 63 & 69] and comparing the third signal [Fig 5A, elts 55 & 62] with the received second signal [Fig 5A, elts 64, 66 & 68] (col 13, line 25 – col 14, line 5).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey, Rodman and Lundkvist with the teachings of Caputo, for the purpose of validating the occurrence of exchanged data without manipulated the actual data. Comparing signals without modification results in faster authentication than to decrypt subsequent validation.

11. Claims 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Rodman et al (U.S. Pat App Pub 2003/0112978 A1), hereinafter referred to as Rodman, in further view of Simon et al (U.S. Pat 5937065 A), hereinafter referred to as Simon.

Re claim 19: The combination of Willey and Rodman teaches all the limitations of claim 14 as previously stated.

However, Simon teaches wherein the authentication check further comprises the step of checking if the identification of the second device is compliant with an expected identification (Fig 3, elts 72, 73, 76 & 80; col 6, lines 36-50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey and Rodman with the teachings of Simon, for the purpose of validating the devices themselves to prevent man-in-the-middle attacks or spoofing.

12. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in view of Rodman et al (U.S. Pat App Pub 2003/0112978 A1), hereinafter referred to as Rodman, in further view of Overy et al (U.S. Pat App Pub 2003/0220765 A1), hereinafter referred to as Overy.

Re claim 22: Willey teaches a system for secure transfer of multimedia content comprising a first communication device in communication with a second communication device, the first communication device comprising:

processing means for (¶34):

securely sharing a common secret with the second communication device if the second communication device is compliant (¶48; ¶56-¶58; *after the exchanged digits are validated, a link key is created, and encrypted using the encryption key and sent to* *the other device where it is decrypted and stored; such common secret is used to establish a secure link*); and

determining a distance measurement between the first and second devices, said distance measurement comprising (Fig 11, elts 200 & 1010; Fig 11a, elts 46 & 48; ¶71; ¶76):

transmitting a spread-spectrum first signal from the first device to the second device at a first time (¶12; Fig 11a, 40; ¶76);

determining the distance based on the difference between the first time and the second time device (Fig 11, elts 200 & 1010; Fig 11a, elts 46 & 48; ¶71; ¶76); and

using the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the multimedia data is transmitted from the first communication device to the second communication device (Fig 11a, elts 48 & 50); and

the second communication device comprising means for playing back the multimedia content (¶8; ¶34; ¶55).

However, Willey does not expressly disclose, yet Rodman teaches said modification being associated with modification of only spreading codes of the spread spectrum first signal (¶19; ¶21-¶23).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey with the teachings of Rodman, for the purpose of providing secured communication between two parties wherein the secured communication is resistant from jamming; spread-spectrum signals have the known utility of providing secure communication resistant to natural interference and deliberate jamming.

The combination of Willey and Rodman does not expressly disclose, yet Overy teaches performing an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device (Fig 4, elts 35 & 36; ¶8-¶9; ¶40).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Willey and Rodman with the teachings of Overy, for the purpose of uniquely identifying devices and preventing unauthorized or unknown devices from joining a protected network.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140

F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

13. Claims 14-19 and 21 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 5-8 and 11 of copending Application No. 10/521858 in view of Rodman et al (U.S. Pat App Pub 2003/0112978 A1), hereinafter referred to as Rodman.

Re instant claim 14:

Instant claim 14	Copending claim 6 (which encompasses the limitations of independent claim 1)
A method of determining whether	A method for a first communication device

multimedia data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of: performing a distance measurement between the first communication device and the second communication device, wherein the first and the second communication device share a common secret which has been shared before performing the distance measurement	to performing authenticated distance measurement between said first communication device and a second communication device, wherein the first and the second communication device share a common secret and wherein the authenticated distance measurement comprises …
performing an authentication check on the second communication device, by checking whether the second communication device is compliant with a set of predefined compliance rules;	performing an authentication check from the first communication device on the second communication device, by checking whether said second communication device is compliant with a set of a predefined compliance rules;
sharing the common secret with the second communication device if the second communication device is compliant; and	if the second communication device is compliant, sharing said common secret by transmitting said secret to the second communication device,
using the common secret after a	wherein the common secret has been

successful authentication check and distance measurement in the generation of a secure authenticated channel.	shared before performing the distance measurement.

The first and second communication devices are synonymous with one-another between the instant and copending claim; this is further held in the distance measurement, common secret and compliance rules.

However, the copending claim does not expressly disclose, yet Rodman teaches the common secret is used to modify only a spreading code of a spread-spectrum communication signal between the first device and the second device (¶17-¶19; ¶21-¶23).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of the copending claim with the teachings of Rodman, for the purpose of providing secured communication between two parties wherein the secured communication is resistant from jamming; spread-spectrum signals have the known utility of providing secure communication resistant to natural interference and deliberate jamming.

Re instant claim 15: Instant claim 15 is rejected as similar in scope to claim 6; the rationale is applied *supra*.

Re instant claim 17: Instant claim 17 is rejected as similar in scope to claim 6 and thus encompasses the subject matter of the combination of both the copending claims and Rodman.

Re instant claim 18: Instant claim 18 is rejected as similar in scope to claim 5 and thus encompasses the subject matter of the combination copending claims and Rodman.

Re instant claim 19: Instant claim 19 is rejected as similar in scope to claim 7 and thus encompasses the subject matter of the combination copending claims and Rodman.

Re instant claim 20: Instant claim 14 is discussed *supra*. Rodman teaches said common secret comprises executing one a key transport protocol and a key agreement protocol (¶19; ¶21-¶23). Thus, the combination of the copending claims and Rodman encompasses the subject matter of the combination copending claims and Rodman.

Re instant claim 21: Instant claim 21 is rejected under provisional obviousness-double patenting as it pertains to copending claims 1, 6 & 11.

This is a provisional obviousness-type double patenting rejection.

14. Claim 22 provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 6 of copending Application No. 10/521858 in view of Rodman et al (U.S. Pat App Pub 2003/0112978 A1), hereinafter referred to as Rodman, in further view of Overy et al (U.S. Pat App Pub 2003/0220765 A1), hereinafter referred to as Overy.

Re instant claim 22: Instant claim 22 with respect to copending claim 6 has been addressed *supra* similar to instant claim 14.

However, the copending claim does not expressly disclose, yet Rodman teaches securely sharing a common secret with the second communication device if the second communication device and said modification being associated with modification of only spreading codes of the spread spectrum first signal (¶19; ¶21-¶23).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of the copending claim with the teachings of Rodman, for the purpose of providing secured communication between two parties wherein the secured communication is resistant from jamming; spread-spectrum signals have the known utility of providing secure communication resistant to natural interference and deliberate jamming.

The combination of the copending claims and Rodman does not expressly disclose, yet Overy teaches performing an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device (Fig 4, elts 35 & 36; ¶8-¶9; ¶40).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of the instant claims and Rodman with the teachings of Overy, for the purpose of uniquely identifying devices and preventing unauthorized or unknown devices from joining a protected network.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTOL-892.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN B. SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 7am-5pm EST, Monday-Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. B. S./
Examiner, Art Unit 2435

/Edward Zee/
Primary Examiner, Art Unit 2435

31

Doc code: RCEX PTO/SB/30EFS (07-09)
Doc description: Request for Continued Examination (RCE)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	12508917	Filing Date	2009-07-24	Docket Number (if applicable)	2002P02007US	Art Unit	2435
First Named Inventor	Frank Kamperman			Examiner Name	D.B. Schwartz		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

□ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

□ Consider the arguments in the Appeal Brief or Reply Brief previously filed on ____________

□ Other ____________

☒ Enclosed

☒ Amendment/Reply

□ Information Disclosure Statement (IDS)

□ Affidavit(s)/ Declaration(s)

□ Other ____________

MISCELLANEOUS

□ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months ____________
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

□ Other ____________

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
Deposit Account No 141270

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

□ Applicant Signature

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Michael E. Belk/	Date (YYYY-MM-DD)	2012-06-01
Name	Michael E. Belk	Registration Number	33357

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Kamperman, Frank.	Attn. No.: 2002P02007 US
SERIAL NO.: 12/508,917	EXAMINER: Schwartz, D.B.
FILED: 07/24/2009	ART UNIT: 2435
	CONFIRMATION No.: 8927

TITLE: SECURE AUTHENTICATED DISTANCE MEASUREMENT

Mail Stop: RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT WITH RCE

Dear Sir:

In response to the Office Action dated 01/05/2012, and the Advisory Action of 03/09/2012, and the Notice of Allowance of 05/10/2012, please amend the application as follows:

IN THE CLAIMS:

Kindly replace the claims of record with the following full set of claims:

1. – 13. (Cancelled)

14. (Currently amended) A method of determining whether ~~multimedia data~~ protected content stored on a first communication device (201, 301) are to be accessed by a second communication device (203, 303), the method comprising the step of:

performing (209) a ~~distance~~ round trip time measurement between the first communication device and the second communication device,

checking whether the round trip time is within a predefined interval, and

allowing access of the protected content provided that the round trip time is within the predefined interval, wherein the round trip time measurement is an authenticated round trip time measurement, and wherein the first and the second communication device share a common secret, and said common secret is used for generating signals used in performing the round trip time measurement in order to authenticate the round trip time measurement between the first and second communication device ~~which has been shared before performing the distance measurement, the method further comprising the steps of:~~

~~performing (205) an authentication check from the first communication device of the second communication device by checking whether the second communication device is compliant with a set of predefined compliance rules;~~

~~securely sharing (207) the common secret with the second communication device if the second communication device is compliant, wherein the common secret is used to modify only a spreading code of a spread-spectrum communication signal between the first device and the second device, wherein the common secret is of a length equal to a chip length of the spreading code;~~

~~transmitting a return signal to the first device wherein the return signal is encoded with the modified spreading code; and~~

- ~~using (211) the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the~~

~~multimedia data is transmitted from the first communication device to the second communication device~~

and wherein:

the first device (201, 301) authenticates the second device (203, 303), the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules, and

the first device (201, 301) securely shares the common secret with the second device (203, 303) according to a key management protocol.

15. (Currently amended) The method according to claim 14, wherein the authenticated ~~distance~~ round trip time measurement ~~further~~ comprises the steps of:

transmitting ~~(309)~~(305) a first signal from the first communication device (201, 301) to the second communication device (203, 303) at a first time t1, the second communication device being adapted ~~(311)~~ for receiving (311) the first signal;

generating (313) a second signal ~~by modifying the received first signal~~ according to the common secret and transmitting (315) the second signal to the first device;

receiving (317) the second signal at a second time t2;

checking (319) if the second signal has been ~~modified~~ generated according to the common secret; and

determining (323) ~~the distance~~ a time difference between the first time t1 and ~~the second communication device according to a time difference between t1 and~~ the second time t2.

16. (Cancelled)

17. (Currently amended) The method according to claim 15, wherein the step of checking (319) if the second signal has been ~~modified~~generated- according to the common secret comprises the steps of:

generating a third signal ~~by modifying the first signal~~ according to the common secret; and

comparing the third signal with the received second signal.

18. (Previously presented) The method according to claim 15, wherein the first signal and the common secret are bit words and where the second signal comprises information being generated by performing an XOR between the bit words.

19. (Currently amended) The method according to claim 14, wherein the authentication check (205) of the second device further comprises the step of checking if the identification of the second device is compliant with an expected identification.

20. (Currently amended) The method according to claim 14, in which ~~the step of sharing (207) said common secret~~ the key management protocol comprises ~~executing~~ one of a key transport protocol and a key agreement protocol.

21. (Currently amended) A first communication device (201, 301, 406) configured for determining whether ~~multimedia data~~ protected content stored on the first communication device are to be accessed by a second communication device (203, 303), the first communication device comprising:

means for performing ~~distance~~ a round trip time measurement between the first communication device (201) and the second communication device (203),

means for checking whether the measured round trip time is within a predefined interval, and wherein the round trip time measurement is an authenticated round trip time measurement, ~~wherein the first communication device comprises~~

a memory storing a common secret, which is ~~securely transmitted to and~~ also stored on the second communication device, said common secret is used for generating signals used in performing the round trip time measurement in order to authenticate the round trip time measurement; ~~said secret being used to modify a spreading code of a spread-spectrum communication signal between the first device and the second device, wherein the common secret is of a length equal to a chip length of the spreading code; the first communication device being configured (403, 411, 413, 417) for sharing the common secret before performing the distance measurement, wherein the first communication device further comprises means for:~~

means for performing (205) an authentication ~~check~~ of the second communication device, ~~by checking whether~~ the authentication of the second device includes verifying that the second ~~communication~~ device ~~is compliant~~ complies with a set of predefined compliance rules; and

means for sharing (207) the common secret with the second communication device if the second communication device is compliant [;]

~~receiving a return signal to the second device wherein the return signal is encoded with the modified spreading code; and~~

~~using (211) the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel and transmitting multimedia data from the first communication device to the second communication device over the secure authenticated channel~~.

22. (Currently amended) A system for secure transfer of ~~multimedia~~ protected content comprising a first communication device (201, 301, 406) in communication with a second communication device (203, 303), the first communication device comprising:

a memory for storing a common secret,

processing means for:

performing a round trip time measurement between the first communication device and the second communication device, and

checking whether the measured round trip time is within a predefined interval, and wherein the round trip time measurement is an authenticated round trip time measurement, the authenticated round trip time measurement being performed using a signal that is generated using the common secret and transmitted between the first and second devices,

performing (205) an authentication ~~check from the first communication device~~ of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device; the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules, securely sharing (207) [a] the common secret with the second communication device if the second communication device is compliant;~~ and~~

~~determining a distance measurement between the first and second devices, said distance measurement comprising:~~

~~transmitting a spread-spectrum first signal from the first device to the second device at a first time, said spread-spectrum first signal having a known spreading code;~~

~~receiving the first signal modified by the common secret at a second time, said modification being associated with modification of the known spreading code of the spread-spectrum first signal wherein the common secret has a bit length equal to a chip length of the known spreading code; and~~

~~determining the distance based on the difference between the first time and the second time; and~~

~~using (211) the common secret after a successful authentication check and distance measurement in the generation of a secure authenticated channel over which the multimedia data is transmitted from the first communication device to the second communication device~~; and

~~the second communication device comprising~~

~~means for playing back~~ transmitting the ~~multimedia~~ protected content to the second device depending on the authenticated round trip time measurement being within the predefined interval.

23. (new) The method according to claim 14, wherein the common secret is securely shared with the second device by encrypting the common secret using a public key of a private/public key-pair.

24. (new) The method according to claim 14, wherein the common secret has been shared before performing the round trip time measurement, the sharing being performed by the steps of,

performing an authentication check (205) from the first communication device (201) on the second communication device (203), by checking whether said second communication device (203) is compliant with a set of predefined compliance rules, if the second communication device is compliant, then sharing (207) said common secret by transmitting said secret to the second communication device (203).

25. (new) The method according to claim 14, wherein the protected content stored on the first device (201) are sent to the second device (203) if it is determined that the protected content stored on the first device (201) are permitted to be shared with the second device (203).

26. (new) The method as in claim 25, wherein the protected content can be sent between the first and the second device after the time difference has been measured in a secure authenticated way.

27. (new) The method according to claim 14, wherein authenticating of the second device (203) by the first device (201) comprises the steps of checking whether the second device (203) is a compliant device.

28. (new) The method according to claim 14, wherein securely sharing the common secret with the second device (203) by the first device (201) comprises transmitting a random generated bit word to the second device (203).

29. (new) The method according to claim 14, wherein the shared common secret is used for generating a secure authenticated channel between the first (201) and the second communication device (203).

30. (new) The first communication device (201) according to claim 21, further comprising

means arranged to securely share the common secret with the second device (203) by encrypting the common secret using a public key of a private/public key-pair.

31. (new) The first communication device (201) according to claim 21, further comprising:

means for transmitting (305) a first signal from the first communication device (201) to the second communication device (203) at a first time t1,

means for receiving (317) a second signal at a second time t2, said second signal being generated according to the common secret,

means for checking (319) if the second signal has been generated according to the common secret,

means for determining (323) a time difference between the first time t1 and the second time t2.

32. (new) The first communication device (201) configured for determining whether protected content stored on a first communication device (201) are to be accessed by a second communication device (203), the second device (203) being adapted for receiving (311) a first signal from the first device, generating (313) a second signal by modifying the received first signal according to a common secret, and transmitting (315) the second signal to the first device, the first device comprising:

a transmitter (411);

a receiver (403);

a memory (305) storing a common secret also stored on the second communication device;

a bus (417) connected to the memory;

a processor (413) connected to the bus and controlling the transmitter and receiver, the processor:

measuring a round trip time between the first (201) and the second communication device (203) and checking whether said measured round trip time is within a predefined interval, the round trip time measurement being an authenticated round trip time measurement, said authenticated round trip time being determined based on said second signal generated according to the common secret, and

authenticating the second device (203), the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules.

33. (new) The first communication device (201) of claim 32 wherein the processor securely shares the common secret with the second communication device by encrypting the common secret using a public key of a private/public key-pair.

34. (new) The first communication device (201) of claim 32 wherein the processor performs the round trip time measurement by: transmitting a first signal from the first device to the second device at time t1, and receiving a second signal from the second device at time t2, checking that the second signal has been generated according to the common secret, and determining a time difference between the first time t1 and the second time t2.

REMARKS

Entry of this Amendment and reconsideration are respectfully requested in view of the above amendments and the following remarks.

Claims 14-15 and 17-34 are pending, and claims 1-13 and 16 are canceled.

Claims 14, 21-22, and 32 are independent claims.

New claims 23-34 have been added. No new matter has been added.

None of the citations suggest an authentication of a second communications device by a first communications device wherein " the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rule" as recited in claims 14, 21-22 and 32.

The claims are amended for non-statutory reasons: to correct one or more informalities, to remove figure label number(s), and/or to replace European-style claim phraseology with American-style claim language.

The amendment to the claims does not address issues of patentability. Applicant(s) reserve(s) the right to continue prosecution of any subject matter canceled, or not claimed, in this, a divisional, or other continuing application.

In addition, Applicant denies any statement, position or averment of the Examiner that is not specifically addressed by the foregoing argument and response. Any rejections and/or points of argument not addressed would appear to be moot in view of the presented remarks. However, the Applicant reserves the right to submit further arguments in support of the above stated position, should that become necessary. No arguments are waived and none of the Examiner's statements are conceded.

In view of the above, it is respectfully submitted that the present application is in condition for allowance, and a Notice of Allowance is earnestly solicited.

If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

The Commissioner is hereby authorized to credit any overpayment or charge any fee (except the issue fee) including fees for any required extension of time, to Account No. 14-1270.

Respectfully submitted.

By /Michael E. Belk/
Michael E. Belk, Reg. 33,357
Senior Patent Attorney
(914) 333-9643

32

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/508,917	07/24/2009	Franciscus Lucas Antonius Johannes KAMPERMAN	2002P02007 US	8927

24737 7590 08/31/2012
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
08/31/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

vera.kublanov@philips.com
debbie.henn@philips.com
marianne.fox@philips.com

Office Action Summary	**Application No.** 12/508,917	**Applicant(s)** KAMPERMAN, FRANCISCUS LUCAS ANTONIUS JO	
	Examiner DARREN B. SCHWARTZ	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 June 2012*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *14,15 and 17-34* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)□ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *14,15 and 17-34* is/are rejected.

8)□ Claim(s) _____ is/are objected to.

9)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)□ The specification is objected to by the Examiner.

11)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *6-13-12*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

In a response filed 01 June 2012, Applicant amends claims 14, 15, 17 & 19-22 and adds claims 23-34.

Claims 14, 15 and 17-34 are presented for examination.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance or after an Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935). Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 01 June 2010 has been entered.

Response to Arguments

Applicant is advised that the Notice of Allowance mailed 10 May 2012 is vacated. If the issue fee has already been paid, applicant may request a refund or request that the fee be credited to a deposit account. However, applicant may wait until the application is either found allowable or held abandoned. If allowed, upon receipt of a new Notice of Allowance, applicant may request that the previously submitted issue fee be applied. If abandoned, applicant may request refund or credit to a specified Deposit Account.

Prosecution on the merits of this application is reopened on claims 14, 15 and 17-34 considered unpatentable for the reasons indicated *infra*.

Applicant's arguments have been carefully considered, but are moot in view of the new grounds of objections and rejections.

Claim Objections

Claims 24, 25 and 27 are objected to because of the following informalities:

Claim 24 recites "from the first communication on the second communication device" and should preferably read: "from the first communication to the second communication device".

Claim 25 recites "protected content stored on the first device are sent to the second device" and should preferably read: "protected content stored on the first device is sent to the second device".

Claim 27 recites "comprises the steps of" and should preferably read: "comprises the step of".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. Claims 27 and 32-34 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 27 recites the limitation "the time difference". There is insufficient antecedent basis for this limitation in the claim.

Claim 32 recites "the processor: measuring … authenticating" and it is unclear as to whether the claim is directed to the device or a method of using the device (*See IPXL Holdings, L.L.C. v. Amazon.Com, Inc.* 430 F.3d 1377, 1384 (Fed. Cir. 2005)). The Examiner believes the claim should preferably read: "the processor configured for: measuring … authenticating".

Any claim not specifically addressed above is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 32 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, in view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist.

Re claim 32: Rofheart teaches The first communication device configured for determining whether protected content stored on a first communication device are to be accessed by a second communication device, the second device being adapted for receiving a first signal from the first device, generating a second signal by modifying the received first signal according to a common secret, and transmitting the second signal to the first device, the first device comprising:

a transmitter (Figs 1 & 2);

a receiver (Figs 1 & 2);

a memory (Fig 2; ¶83-¶91); a bus connected to the memory (Fig 2; ¶83-¶91);

a processor connected to the bus and controlling the transmitter and receiver (Fig 1; Fig 2; ¶83-¶91), the processor:

measuring a round trip time between the first and the second communication device and checking whether said measured round trip time is within a predefined interval, the round trip time measurement being an authenticated round trip time measurement (Fig 6, elts 603 & 605; ¶117-¶118; Fig 8, elts 803, 805 & 807; ¶136; *Rofheart teaches determining the distance between two devices falls within the set of authentication criteria, e.g.* $D<r$, $r1<D<R2$ *or* $D=R$*; the distance D is calculated via the formula* $D = C \times Trt/2$; *ergo, to satisfy the authentication criteria, one of the following must validate successfully:* $Trt < 2 \times r/C$, $2 \times r1/C < Trt < 2 \times R2/C$ or $Trt = 2 \times R/C$),

authenticating the second device, the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules (Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*).

However, Rofheart does not expressly disclose, yet,

Lundkvist teaches a memory storing a common secret [*O_RND; E_RND*] also stored on the second communication device (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50); said authenticated round trip time being determined based on said second signal generated according to the common secret (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

Re claim 34: The combination of Rofheart and Lundkvist teaches the processor performs the round trip measurement by: transmitting a first signal from the first device to the second device at time t1, and receiving a second signal from the second device at time t2, and determining a time difference between the first time t1 and the second time t2 (Rofheart: Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134).

The combination further teaches checking that the second signal [Lundkvist: Fig 2, elt Y1; Fig 3, elts Z & Y2; Fig 4, elt Y3; Fig 5, elt Y4] has been generated according to the common secret [Lundkvist: *O_RND; E_RND*] (Lundkvist: Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of

Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

3. Claims 14, 15, 19, 20 and 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, in view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, in further view of Kronenberg (U.S. Pat App Pub 2002/0078227 A1), hereinafter referred to as Kronenberg.

<u>Re claim 1</u>: Rofheart teaches a method of determining whether protected content stored on a first communication device are to be accessed by a second communication device, the method comprising the step of:

performing a round trip time measurement between the first communication device and the second communication device (Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134),

checking whether the round trip time is within a predefined interval (Fig 6, elts 603 & 605; ¶117-¶118; Fig 8, elts 803, 805 & 807; ¶136; *Rofheart teaches determining the distance between two devices falls within the set of authentication criteria, e.g. D<r, r1<D<R2 or D=R; the distance D is calculated via the formula D = C ×* Trt/2; *ergo, to satisfy the authentication criteria, one of the following must validate successfully: Trt < 2×r/C, 2×*r1/C < Trt < 2×R2/C or Trt = 2×R/C), and allowing access of the protected content provided that the round trip time is within the predefined interval, wherein the round trip time measurement is an authenticated round trip time measurement (Fig 6, elts 605 – satisfied → 609 → 611; ¶118; ¶122; Fig 8, elts 807 – satisfied → 811 → 813 → 815; ¶135-¶136; ¶138),

the first device authenticates the second device, the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules (Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*).

However, Rofheart does not expressly disclose, yet,

Lundkvist teaches wherein the first and the second communication device share a common secret [*O_RND; E_RND*] (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50), and said common secret [*O_RND; E_RND*] is used for generating signals used in performing the round trip time measurement in order to authenticate the round trip time measurement between the first and second communication device (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of

messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

The combination of Rofhert and Lundkvist does not expressly disclose, yet,

Kronenberg teaches the first device securely shares the common secret with the second device according to a key management protocol (¶9).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart and Lundkvist with the teachings of Kronenberg, for the purpose of protecting both the confidentiality of exchanged information, but also the authenticity of exchanged information for the known purpose of providing non-repudiation and resistance to tampering of such information.

<u>Re claim 15</u>: The combination of Rofheart, Lundkvist and Kronenberg teaches wherein the authenticated round trip time measurement comprises the steps of: transmitting a first signal from the first communication device to the second communication device at a first time t1, the second communication device being adapted for receiving the first signal; generating a second signal and transmitting the second signal to the first device; receiving the second signal at a second time t2; determining a time different between the first time t1 and the second time t2 (Rofheart: Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134).

The combination further teaches generating a second signal [Lundkvist: Fig 2, elt Y1; Fig 3, elts Z & Y2; Fig 4, elt Y3; Fig 5, elt Y4] according to the common secret [Lundkvist: *O_RND; E_RND*] and checking if the second signal has been generated according to the common secret (Lundkvist: Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

Re claim 19: The combination Rofheart, Lundkvist and Kronenberg teaches of wherein the authentication check of the second device further comprises the step of checking if the identification of the second device is compliant with an expected identification (Rofheart: Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*).

Re claim 20: The combination Rofheart, Lundkvist and Kronenberg teaches the key management protocol comprises one of a key transport protocol and a key agreement protocol (Kronenberg: ¶9).

Re claim 25: The combination Rofheart, Lundkvist and Kronenberg teaches the protected content stored on the first device are sent to the second device if it is determined that the protected content stored on the first device are permitted to be shared with the second device (Rofheart: Fig 6, elts 605 – satisfied → 609 → 611; ¶118; ¶122; Fig 8, elts 807 – satisfied → 811 → 813 → 815; ¶135-¶136; ¶138),

Re claim 26: The combination Rofheart, Lundkvist and Kronenberg teaches the protected content can be sent between the first and the second device after the time difference has been measured in a secure authenticated way (Rofheart: Fig 6, elts 605 – satisfied → 609 → 611; ¶118; ¶122; Fig 8, elts 807 – satisfied → 811 → 813 → 815; ¶135-¶136; ¶138),

Re claim 27: The combination Rofheart, Lundkvist and Kronenberg teaches authenticating of the second device by the first device comprises the steps of checking whether the second device is a compliant device (Rofheart: Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*).

Re claim 28: The combination Rofheart, Lundkvist and Kronenberg teaches securely sharing the common secret with the second device by the first device comprises transmitting a random generated bit word [Lundkvist: *O_RND; E_RND*] to the second device (Lundkvist: Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

4. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as

Rofheart, Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, and Kronenberg (U.S. Pat App Pub 2002/0078227 A1), hereinafter referred to as Kronenberg, in further view of Caputo et al (U.S. Pat 5778071 A), hereinafter referred to as Caputo.

Re claim 17: The combination of Rofheart, Lundkvist and Kronenberg teaches the step of checking if the second signal [Lundkvist: Fig 2, elt Y1; Fig 3, elts Z & Y2; Fig 4, elt Y3; Fig 5, elt Y4] has been generated according to the common secret (Lundkvist: ¶31-¶34; ¶36-¶38; ¶44-¶49).

Caputo teaches the step of checking if the second signal [Fig 5A, elts 60→70→68→66] has been generated according to the common secret [Fig 5A, elts *random number generated; user PIN*] (Fig 5A, elt 64; col 13, line 25 – col 14, line 8);

generating a third signal [Fig 5A, elts 54→55→62] according to the common secret [Fig 5A, elts *random number generated; user PIN*] and comparing the third signal [Fig 5A, elt 62] with the received second signal [Fig 5A, elt 66] (Fig 5A, elt 64; col 13, line 25 – col 14, line 8).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist and Kronenberg with the teachings of Caputo, for the purpose of authenticating a received signal without altering the signal received; such reduces risks associated with data corruption by decreasing the number of operations acted upon the data received. Also Caputo further improves upon the teachings of the combination of Rofheart, Lundkvist and Kronenberg by also authenticating what a user knows, a.k.a. a PIN, before establishing a secure communication, thus further tightening security of the communication system.

Re claim 18: The combination of Rofheart, Lundkvist and Kronenberg does not expressly disclose, yet,

Caputo teaches the first signal [Fig 5A, elts 54→56→58] and the common secret [Fig 5A, elts *random number generated; user pint*] are bit words and where the second signal comprises information being generated by performing an XOR between the bit words (Fig 5A, elts 60 & 70; line 25 – col 14, line 8).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist and Kronenberg with the teachings of Caputo, for the purpose of authenticating a received signal without altering the signal received; such reduces risks associated with data corruption by decreasing the number of operations acted upon the data received. Also Caputo further improves upon the teachings of the combination of Rofheart, Lundkvist and Kronenberg by also authenticating what a user knows, a.k.a. a PIN, before establishing a secure communication, thus further tightening security of the communication system. Additionally, exclusive-or encryption has the known utility of being both a fast cipher with a high level of protection, as is known in the art.

5. Claims 21 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, in view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter

referred to as Lundkvist, in further view of Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey.

Re claim 21: Rofheart teaches a first communication device (Fig 3, elts 302, 303 & 303N) configured for determining whether protected content stored on the first communication device are to be accessed by a second communication device (Fig 3, elt 301), the first communication device comprising:

means for [¶103] performing a round trip time measurement between the first communication device and the second communication device (Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134),

means for [¶103] checking whether the measured round trip time is within a predefined interval (Fig 6, elts 603 & 605; ¶117-¶118; Fig 8, elts 803, 805 & 807; ¶136; *Rofheart teaches determining the distance between two devices falls within the set of authentication criteria, e.g. D<r, r1<D<R2 or D=R; the distance D is calculated via the formula D = C* × Trt/2; *ergo, to satisfy the authentication criteria, one of the following must validate successfully: Trt < 2×r/C, 2*×r1/C < Trt < 2×R2/C or Trt = 2×R/C), and

wherein the round trip time measurement is an authenticated round trip time measurement (Fig 6, elts 605 – satisfied → 609 → 611; ¶118; ¶122; Fig 8, elts 807 – satisfied → 811 → 813 → 815; ¶135-¶136; ¶138).

However, Rofheart does not expressly disclose, yet,

Lundkvist teaches:

a memory storing a common secret [*O_RND; E_RND*] (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50), which is also stored on the second communication device, said common secret is used for generating signals used in performing the round trip time measurement in order to authenticate the round trip time measurement (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

However, the combination of Rofheart and Lundkvist does not expressly disclose, yet,

Willey teaches:

means for [Fig 6, elts 100 & 300] performing an authentication of the second communication device, the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules (Fig 5a, elt 6; ¶48-¶49); and

means for [Fig 6, elts 100 & 300] sharing the common secret with the second communication device if the second communication device is compliant (Fig 5a, elts 6—Yes→7; ¶48-¶49).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart and Lundkvist with the teachings of Willey, for the purpose of mutually authenticating the communicating the devices before sharing confidential data to prevent unauthorized snooping or linking of devices.

Re claim 31: The combination of Rofheart, Lundkvist and Willey teaches means for [¶103] transmitting a first signal from the first communication device to the second communication device at a first time t1, means for [¶103] receiving a second signal at a second time t2, means for determining a time difference between the first time t1 and the second time t2 (Rofheart: Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134).

The combination further teaches said second signal [Lundkvist: Fig 2, elt Y1; Fig 3, elts Z & Y2; Fig 4, elt Y3; Fig 5, elt Y4] according being generated according to the common secret [Lundkvist: *O_RND; E_RND*], means for [Fig 1, elts 1 & 2] checking if the second signal has been generated according to the common secret (Lundkvist: Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of

messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

6. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, and Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in further view of Kaliski, Jr. (U.S. Pat 6085320 A), hereinafter referred to as Kaliski.

Re claim 30: The combination of Rofheart, Lundkvist and Willey teaches all the limitations of claim 21 as previously stated.

Kaliski teaches means arranged to [Fig 1; Fig 4A, elts 20 & 40] securely share the common secret [Figs 3A & 3B: elt *session key KSS*] with the second device by encrypting the common secret [Figs 3A & 3B: elt *session key KSS*] using a public key [Figs 3A & 3B: elt PUB_{SERV}] of a private/public key-pair [Figs 3A & 3B: elts PUB_{SERV} *and* $PRIV_{SERV}$] (Figs 3A & 3B; col 4, line 32 – col 5, line 29).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist and Willey with the teachings of Kaliski, for the purpose of protecting the symmetric key from unauthorized exposure; using key-encrypting-key techniques, specifically transmitting an encrypted symmetric key via encrypting the symmetric key with a public key and decrypting the received encrypted symmetric key via a private key of the public key was well known in the art of secure key distribution. Such incorporation of key-encrypting-key techniques of Kaliski into the combination of Rofheart, Lundkvist and Willey supplies these well-known utilities.

7. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, and Kronenberg (U.S. Pat App Pub 2002/0078227 A1), hereinafter referred to as Kronenberg, in further view of Kaliski, Jr. (U.S. Pat 6085320 A), hereinafter referred to as Kaliski.

Re claim 23: The combination of Rofheart, Lundkvist and Kronenberg teaches all the limitations of claim 14 as previously stated.

Kaliski teaches the common secret [Figs 3A & 3B: elt *session key KSS*] is securely shared with the second device by encrypting the common secret [Figs 3A & 3B: elt *session key KSS*] using a public key [Figs 3A & 3B: elt PUB_{SERV}] of a private/public key-pair [Figs 3A & 3B: elts PUB_{SERV} *and* $PRIV_{SERV}$] (Figs 3A & 3B; col 4, line 32 – col 5, line 29).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist and Willey with the teachings of Kaliski, for the purpose of protecting the symmetric key from unauthorized exposure; using key-encrypting-key techniques, specifically transmitting an encrypted symmetric key via encrypting the symmetric key with a public key and decrypting the received encrypted symmetric key via a private key of the public key was well known in the art of secure key distribution. Such incorporation of key-encrypting-key techniques of Kaliski into the combination of Rofheart, Lundkvist and Willey supplies these well-known utilities.

8. Claims 24 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, and Kronenberg (U.S. Pat App Pub 2002/0078227 A1), hereinafter referred to as Kronenberg, in further view of Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey.

Re claim 24: The combination of Rofheart, Lundkvist and Kronenberg teaches all the limitations of claim 14 as previously stated and further teaches the common secret has been shared before performing the round trip time measurement (Fig 2, elts & "X is sent" & X; Fig 3, elts "X is sent" & X; Fig 4, elts X1, Z1, X2, Z2, X3, Xn & Zn)

However, the combination of Rofheart, Lundkvist and Kronenberg does not expressly disclose, yet,

Willey teaches the sharing being performed by the steps of, performing an authentication check from the first communication device on the second communication device, by checking whether said second communication device is compliant with a set of predefined compliance rules, if the second communication device is compliant, then sharing said common secret by transmitting said secret to the second communication device (Fig 5a, elts 6—Yes→7; ¶48-¶49).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist and Kronenberg with the teachings of Willey, for the purpose of mutually authenticating the communicating the devices before sharing confidential data to prevent unauthorized snooping or linking of devices.

Re claim 29: The combination Rofheart, Lundkvist and Kronenberg teaches all the limitations of claim 14 as previously stated.

Willey teaches the shared common secret is used for generating a secure authenticated channel between the first and the second communication device (Fig 5a; ¶48-¶49).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist and Kronenberg with the teachings of Willey, for the purpose of mutually authenticating the communicating the devices before sharing confidential data to prevent unauthorized snooping or linking of devices.

9. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, in view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, and Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in further view of Traw et al (U.S. Pat 5949877 A), hereinafter referred to as Traw.

Re claim 22: Rofheart teaches a system for secure transfer of protected content comprising a first communication device in communication with a second communication device, the first communication device (Fig 3, elts 302, 303 & 303N) comprising:

processing means for [Fig 3, ¶102-¶103]:

performing a round trip time measurement between the first communication device and the second communication device (Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134), and

checking whether the measured round trip time is within a predefined interval, and wherein the round trip time measurement is an authenticated round trip time measurement, the authenticated round trip time measurement being performed using a signal that is generated and transmitted between the first and second devices (Fig 6, elts 603 & 605; ¶117-¶118; Fig 8, elts 803, 805 & 807; ¶136; *Rofheart teaches determining the distance between two devices falls within the set of authentication criteria, e.g. D<r, r1<D<R2 or D=R; the distance D is calculated via the formula D = C* × Trt/2; *ergo, to satisfy the authentication criteria, one of the following must validate successfully: Trt < 2×r/C, 2*×r1/C < Trt < 2×R2/C or Trt = 2×R/C);

performing an authentication of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device (Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and* *determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*); the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules (Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*),

transmitting the protected content to the second device depending on the authenticated round trip time measurement being within the predefined interval (Fig 6, elts 605 – satisfied → 609 → 611; ¶118; ¶122; Fig 8, elts 807 – satisfied → 811 → 813 → 815; ¶135-¶136; ¶138).

However, Rofheart does not expressly disclose, yet,

Lundkvist teaches

a memory for storing a common secret [*O_RND; E_RND*] (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50),

the authenticated round trip time measurement being performed using a signal that is generated using the common secret (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

However, Rofheart and Lundkvist does not expressly disclose, yet,

Willey teaches securely sharing the common secret with the second communication device if the second communication device is compliant (Fig 5a, elts 6—Yes→7; ¶48-¶49).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart and Lundkvist with the teachings of Willey, for the purpose of mutually authenticating the communicating the devices before sharing confidential data to prevent unauthorized snooping or linking of devices.

However, the combination of Rofheart, Lundkvist and Willey does not expressly disclose, yet,

Traw teaches said identification being based on a certificate in the second device (Fig 1a, elt 112; Fig 1b, elt 116; Fig 1c, elt 130 & 134; col 6, lines 25-35; col 7, lines 5-65).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist and Willey with the teachings of Traw, for the purpose of validating compliancy of each device and cryptographically tying the device identification information to the device itself via a digital certificate, as is taught by Traw.

10. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, in view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, in further view of Kaliski, Jr. (U.S. Pat 6085320 A), hereinafter referred to as Kaliski.

Re claim 33: The combination of Rofheart and Lundkvist teaches all the limitations of claim 32 as previously stated.

Kaliski teaches wherein the processor [Fig 1; Fig 4A, elts 20 & 40] securely share the common secret [Figs 3A & 3B: elt *session key KSS*] with the second device by encrypting the common secret [Figs 3A & 3B: elt *session key KSS*] using a public key [Figs 3A & 3B: elt PUB_{SERV}] of a private/public key-pair [Figs 3A & 3B: elts PUB_{SERV} *and* $PRIV_{SERV}$] (Figs 3A & 3B; col 4, line 32 – col 5, line 29).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart and Lundkvist with the teachings of Kaliski, for the purpose of protecting the symmetric key from unauthorized exposure; using key-encrypting-key techniques, specifically transmitting an encrypted symmetric key via encrypting the symmetric key with a public key and decrypting the received encrypted symmetric key via a private key of the public key was well known in the art of secure key distribution. Such incorporation of key-encrypting-key techniques of Kaliski into the combination of Rofheart and Lundkvist supplies these well-known utilities.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 14, 15 and 17-34 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 3, 5-11 and 13 of copending Application No. 10/521858.

This is a provisional obviousness-type double patenting rejection.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN B. SCHWARTZ whose telephone number is

(571)270-3850. The examiner can normally be reached on 7am-5pm EST, Monday-Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/DARREN B SCHWARTZ/
Primary Examiner, Art Unit 2435

33

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/508,917	07/24/2009	Franciscus Lucas Antonius Johannes KAMPERMAN	2002P02007 US	8927

24737 7590 01/04/2013
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
01/04/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

vera.kublanov@philips.com
debbie.henn@philips.com
marianne.fox@philips.com

Office Action Summary	**Application No.** 12/508,917	**Applicant(s)** KAMPERMAN, FRANCISCUS LUCAS ANTONIUS JO	
	Examiner Darren B. Schwartz	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2012*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *14,15 and 17-34* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)□ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *14,15 and 17-34* is/are rejected.

8)□ Claim(s) _____ is/are objected to.

9)□ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)□ The specification is objected to by the Examiner.

11)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

3) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

4) □ Other: _____.

Examiner-Initiated Interview Summary	**Application No.** 12/508,917	**Applicant(s)** KAMPERMAN, FRANCISCUS LUCAS ANTONIUS JO	
	Examiner Darren B. Schwartz	**Art Unit** 2435	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Darren B. Schwartz*. (3)_____.

(2) *Mr. Carl A. Giordano*. (4)_____.

Date of Interview: *17 December 2012*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *14*.

Identification of prior art discussed: *Rofheart et al, Lundkvist, Kronenberg and Willey*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

This interview summary represents a series of interviews between the Examiner and Applicant's Representative. The Examiner indicated to Applicant's Representative that the claim amendments did not overcome the art of record as presented and as amended. The Examiner recommended further clarification of claim terminology, specifically, the claimed compliance, a set of predefined compliance rules and authenticating the second device. These avenues did not yielded additional subject matter or distinguish pending subject matter over the art of record. The Examiner indicated the Willey reference potentially taught such subject matter where such a reference had been presented in prosecution. Since no agreement could be reached, Applicant urged the Examiner to issue an action on the merits memorializing the Examiner's position; accordingly, the Office Action accompanying this document is entered.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/Darren B Schwartz/
Primary Examiner, Art Unit 2435

DETAILED ACTION

In a response filed 30 November 2012, Applicant amends claims 14, 24-27 and 32.

Claims 14, 15 and 17-34 are presented for examination.

Response to Arguments

1. In light of Applicant's amendments to the claims, the claim objections are withdrawn.

2. In light of Applicant's amendments to the claims, the claim rejections under 35 U.S.C. 112(2) are withdrawn.

Applicant's arguments with respect to claims 14, 15, 17-20, 23-29 and 32-34 have been considered but are moot in view of the new grounds of rejections. As necessitated by Applicant's amendments to the claims, the Examiner further applies Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey.

Applicant's arguments filed with respect to claims 21, 22 and 30-34 have been fully considered but they are not persuasive.

3. On page 11 of Remarks, Applicant argues: "Applicant respectfully disagrees with and explicitly traverses the rejections of the claims. However, in order to provide further clarity to the subject matter claimed as the invention, the independent claims 1 and 32

have been amended to further recite that the common secret is transmitted after the second device has been authenticated in satisfying a predetermined set of compliance rules."

It is noted that mere disagreement does not constitute a separate argument for patentability.

4. On pages 11-12 of Remarks, Applicant addresses the teachings of Lundkvist.

The Examiner in no way subscribes to applicant's characterization or summarization of the art of record.

5. On pages 12-13 of Remarks, Applicant addresses various precedence and caselaw addressing positions of obviousness; Applicant further incorporates "[T]here must be some reason for the combination other than the hindsight gained from the invention, i.e., something in the prior art as a whole must suggest the desirability and thus the obviousness of making the combination." *Uniroyal Inc. v. Rudlkin-Wiley Corp* (citation omitted) [837 F.2d 1044, decided 13 January 1988]."

While the Examiner concurs with Applicant insofar that each limitation must be suggested by the art, obviousness may be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988), *In re Jones*, 958 F.2d 347, 21

USPQ2d 1941 (Fed. Cir. 1992), and *KSR International Co. v. Teleflex, Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). Accordingly, Examiners are not held to the strict standard suggested by *Uniroyal*.

6. On page 14 of Remarks, Applicant argues: "Rather, as disclosed above, Lundkvist discloses that the object and the portable device each must possess the common secret (assuming that encryption disclosed by Lundkvist is performed using a common secret and not just a public/private key) before the portable device is determined to be compliant. Thus, even if the security protocols of Kronenberg were incorporated into the teachings of Rofheart and Lundkvist, the combination would require that the common secret exchange based on Kronenberg is performed prior to the first signal is transmitted from the object to the portable device (Rofheart, Lundkvist) so that the protable device may have the common secret prior to the encryption process. According (*sic*), the combination of Rofheart, Lundkvist and Kronenberg fails to disclose the element of 'means for sharing (207) the common secret with the second communication device if the second communication device is compliant."

As an initial matter, the Examiner notes that such language is not recited in claims 14, 15, 19, 20 and 25-28; thus, the Examiner assumes the argument is actually addressing claim 21 which recites "means for sharing (207) the common secret with the second communication device if the second communication device is compliant."

However, the Examiner rejected claim 21 in view of the combination of Rofheart, Lundkvist and Willey where the Willey reference was applied as teaching the claimed means for sharing; accordingly, Applicant has not addressed the Examiner's actual position.

7. On page 15 of Remarks, Applicant argues: “In addition, the Office Action refers to Willey for teaching means for performing an authentication and means for sharing the common secret with the second device if the second device is compliant. (see Fig. 5a, elts 6-Yes – 7; Para. 0048-0049). Applicant respectfully disagrees with and explicitly traverses the rejection of the claims. With reference to para. 0049, Willey discloses that ‘public keys are exchanged and a shared secret and an antispoof variable 36 are computed in each device.’ Hence, Willey discloses that the shared secret is computed by each device and not ‘means for sharing (207) the common secret with the second communication device if the second communication device is compliant.’”

The Examiner disagrees and notes that the Examiner previously addressed the Willey reference (see final Rejection 05 January 2012 at pages 3 & 4 along with the Advisory Action 05 May 2011).

The position is duplicated where it was stated: The Examiner notes the following has been held: “All of the disclosures in a reference must be evaluated for what they fairly teach one of ordinary skill in the art.” *In re Lemelson*, 397 F.2d 1006, 1009 (CCPA 1968). “The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain.” (quoting *In re Boe*, 355 F.2d 961, 965 (CCPA 1966)).

Willey explicitly states:

> "If the user 400 does not give positive confirmation on both devices 100 and 300 or if the user 400 indicates a mismatch between digits, the pairing can be aborted, or it can be restarted with a new key agreement. After the user 400 has given positive confirmation on both the headset 300 and the handset 100, then the devices 100 and 300 are fully authenticated. In the next step 7, the devices 100 and 300 securely establish the link key. For example, the devices 100, 300 can both derive a symmetric encryption key based upon the elliptic curve Diffie-Hellman shared secret. A link key is created, and encrypted using the encryption key and send to the other device 300 which decrypts and stores it. The link key is then be used by the devices 100 and 300 for BLUETOOTH authentication and encryption. Alternately, a long PIN may be sent from one device 100 to the other encrypted with the encryption key. The other device 300 would then decrypt it and then the devices 100 and 300 would establish a link key based upon a shared PIN using the well-known BLUETOOTH procedure." (¶48 with emphasis added by Examiner).

The Examiner notes that "compliance" is defined as "conformity in fulfilling official requirements" (Webster's Ninth New Collegiate Dictionary, Merriam Webster, 1991).

Accordingly, the validation of the digits between the pairing device in Figure 5a, element 6 can be broadly interpreted as authenticating both devices which can be broadly, yet reasonably interpreted as validating compliance of each device. Such validation of the digits of both devices teaches a predefined compliance rule and thus teaches, at least, a set of predefined compliance rules. Subsequent to such positive authentication, the link key is shared by encrypting the link key with an encryption key and subsequently decrypting the link key using the encryption key at the receiving device. Such steps of securely sharing the link key is predicated if-and-only-if Figure 5A, element 6 matches the digits displayed on both devices which teaches the claimed means for sharing the common secret with the second communication device fi the second communication device is compliant.

8. On pages 16-17 of Remarks, Applicant argues: “With regard to the rejection of the claims under the judicially created doctrine of double patenting, applicant respectfully requests that this rejection be held in abeyance until such time that this application or the referred to application issues and the claims in the current application may be compared to the issued claims to determine if the rejection is still applicable."

Accordingly, the claim rejections under the judicially created doctrine of double patenting is sustained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 14, 15, 19, 20 and 24-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, and Kronenberg (U.S. Pat App Pub 2002/0078227 A1), hereinafter referred to as Kronenberg, in further view of Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey.

Re claim 14: Rofheart teaches a method of determining whether protected content stored on a first communication device are to be accessed by a second communication device, the method comprising the step of:

performing a round trip time measurement between the first communication device and the second communication device (Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134),

checking whether the round trip time is within a predefined interval (Fig 6, elts 603 & 605; ¶117-¶118; Fig 8, elts 803, 805 & 807; ¶136; *Rofheart teaches determining the distance between two devices falls within the set of authentication criteria, e.g.* $D<r$, $r1<D<R2$ *or* $D=R$; *the distance D is calculated via the formula* $D = C \times Trt/2$; *ergo, to satisfy the authentication criteria, one of the following must validate successfully:* $Trt < 2\times r/C$, $2\times r1/C < Trt < 2\times R2/C$ or $Trt = 2\times R/C$), and

allowing access of the protected content provided that the round trip time is within the predefined interval, wherein the round trip time measurement is an authenticated round trip time measurement (Fig 6, elts 605 – satisfied → 609 → 611; ¶118; ¶122; Fig 8, elts 807 – satisfied → 811 → 813 → 815; ¶135-¶136; ¶138), the first device authenticates the second device, the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules (Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*).

However, Rofheart does not expressly disclose, yet,

Lundkvist teaches wherein the first and the second communication device share a common secret [*O_RND; E_RND*] (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50), and said common secret [*O_RND; E_RND*] is used for generating signals used in performing the round trip time measurement in order to authenticate the round trip time measurement between the first and second communication device (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

The combination of Rofheart and Lundkvist does not expressly disclose, yet, Kronenberg teaches the first device securely shares the common secret with the second device according to a key management protocol (¶9).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart and Lundkvist with the teachings of Kronenberg, for the purpose of protecting both the confidentiality of exchanged information, but also the authenticity of exchanged information for the known purpose of providing non-repudiation and resistance to tampering of such information.

The combination of Rofheart, Lundkvist, and Kronenberg does not expressly disclose, yet,

Wiley teaches the first device securely shares the common secret with the second device after having authenticated the second device (Fig 5a, elts 6—Yes→7; ¶48-¶49).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist, and Kronenberg with the teachings of Willey, for the purpose of mutually authenticating the communicating the devices before sharing confidential data to prevent unauthorized snooping or linking of devices.

Re claim 15: The combination of Rofheart, Lundkvist, Kronenberg and Willey teaches wherein the authenticated round trip time measurement comprises the steps of: transmitting a first signal from the first communication device to the second communication device at a first time t1, the second communication device being adapted for receiving the first signal; generating a second signal and transmitting the second signal to the first device; receiving the second signal at a second time t2; determining a time different between the first time t1 and the second time t2 (Rofheart: Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134).

The combination further teaches generating a second signal [Lundkvist: Fig 2, elt Y1; Fig 3, elts Z & Y2; Fig 4, elt Y3; Fig 5, elt Y4] according to the common secret [Lundkvist: *O_RND; E_RND*] and checking if the second signal has been generated according to the common secret (Lundkvist: Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

Re claim 19: The combination Rofheart, Lundkvist, Kronenberg and Willey teaches of wherein the authentication check of the second device further comprises the step of checking if the identification of the second device is compliant with an expected identification (Rofheart: Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*).

Re claim 20: The combination Rofheart, Lundkvist, Kronenberg and Willey teaches the key management protocol comprises one of a key transport protocol and a key agreement protocol (Kronenberg: ¶9).

Re claim 24: The combination Rofheart, Lundkvist, Kronenberg and Willey teaches the common secret has been shared before performing the round trip time measurement (Fig 2, elts & "X is sent" & X; Fig 3, elts "X is sent" & X; Fig 4, elts X1, Z1, X2, Z2, X3, Xn & Zn); and sharing being performed by the steps of, performing an authentication check from the first communication device on the second communication device, by checking whether said second communication device is compliant with a set of predefined compliance rules, if the second communication device is compliant, then sharing said common secret by transmitting said secret to the second communication device (Willey: Fig 5a, elts 6—Yes→7; ¶48-¶49).

Re claim 25: The combination Rofheart, Lundkvist, Kronenberg and Willey teaches the protected content stored on the first device are sent to the second device if it is determined that the protected content stored on the first device are permitted to be shared with the second device (Rofheart: Fig 6, elts 605 – satisfied → 609 → 611; ¶118; ¶122; Fig 8, elts 807 – satisfied → 811 → 813 → 815; ¶135-¶136; ¶138),

Re claim 26: The combination Rofheart, Lundkvist, Kronenberg and Willey teaches the protected content can be sent between the first and the second device after the time difference has been measured in a secure authenticated way (Rofheart: Fig 6, elts 605 – satisfied → 609 → 611; ¶118; ¶122; Fig 8, elts 807 – satisfied → 811 → 813 → 815; ¶135-¶136; ¶138), Re claim 27: The combination Rofheart, Lundkvist, Kronenberg and Willey teaches authenticating of the second device by the first device comprises the steps of checking whether the second device is a compliant device (Rofheart: Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*).

Re claim 28: The combination Rofheart, Lundkvist, Kronenberg and Willey teaches securely sharing the common secret with the second device by the first device comprises transmitting a random generated bit word [Lundkvist: *O_RND; E_RND*] to the second device (Lundkvist: Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

Re claim 29: The combination Rofheart, Lundkvist, Kronenberg and Willey teaches the shared common secret is used for generating a secure authenticated channel between the first and the second communication device (Willey: Fig 5a; ¶48-¶49).

10. Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, Kronenberg (U.S. Pat App Pub 2002/0078227 A1), hereinafter referred to as Kronenberg, and Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as

Willey, in further view of Caputo et al (U.S. Pat 5778071 A), hereinafter referred to as Caputo.

Re claim 17: The combination of Rofheart, Lundkvist, Kronenberg and Willey teaches the step of checking if the second signal [Lundkvist: Fig 2, elt Y1; Fig 3, elts Z & Y2; Fig 4, elt Y3; Fig 5, elt Y4] has been generated according to the common secret (Lundkvist: ¶31-¶34; ¶36-¶38; ¶44-¶49).

Caputo teaches the step of checking if the second signal [Fig 5A, elts 60→70→68→66] has been generated according to the common secret [Fig 5A, elts *random number generated; user PIN*] (Fig 5A, elt 64; col 13, line 25 – col 14, line 8);

generating a third signal [Fig 5A, elts 54→55→62] according to the common secret [Fig 5A, elts *random number generated; user PIN*] and comparing the third signal [Fig 5A, elt 62] with the received second signal [Fig 5A, elt 66] (Fig 5A, elt 64; col 13, line 25 – col 14, line 8).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist, Kronenberg and Willey with the teachings of Caputo, for the purpose of authenticating a received signal without altering the signal received; such reduces risks associated with data corruption by decreasing the number of operations acted upon the data received. Also Caputo further improves upon the teachings of the combination of Rofheart, Lundkvist, Kronenberg and Willey by also authenticating what a user knows, a.k.a. a PIN, before establishing a secure communication, thus further tightening security of the communication system.

Re claim 18: The combination of Rofheart, Lundkvist, Kronenberg and Willey does not expressly disclose, yet,

Caputo teaches the first signal [Fig 5A, elts 54→56→58] and the common secret [Fig 5A, elts *random number generated; user pint*] are bit words and where the second signal comprises information being generated by performing an XOR between the bit words (Fig 5A, elts 60 & 70; line 25 – col 14, line 8).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist, Kronenberg and Willey with the teachings of Caputo, for the purpose of authenticating a received signal without altering the signal received; such reduces risks associated with data corruption by decreasing the number of operations acted upon the data received. Also Caputo further improves upon the teachings of the combination of Rofheart, Lundkvist, Kronenberg and Willey by also authenticating what a user knows, a.k.a. a PIN, before establishing a secure communication, thus further tightening security of the communication system. Additionally, exclusive-or encryption has the known utility of being both a fast cipher with a high level of protection, as is known in the art.

11. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, Kronenberg (U.S. Pat App Pub 2002/0078227 A1), hereinafter referred to as Kronenberg, and Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as

Willey, in further view of Kaliski, Jr. (U.S. Pat 6085320 A), hereinafter referred to as Kaliski.

Re claim 23: The combination of Rofheart, Lundkvist, Kronenberg and Willey teaches all the limitations of claim 14 as previously stated.

Kaliski teaches the common secret [Figs 3A & 3B: elt *session key KSS*] is securely shared with the second device by encrypting the common secret [Figs 3A & 3B: elt *session key KSS*] using a public key [Figs 3A & 3B: elt *PUB_{SERV}*] of a private/public key-pair [Figs 3A & 3B: elts *PUB_{SERV} and $PRIV_{SERV}$*] (Figs 3A & 3B; col 4, line 32 – col 5, line 29).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist, Kronenberg and Willey with the teachings of Kaliski, for the purpose of protecting the symmetric key from unauthorized exposure; using key-encrypting-key techniques, specifically transmitting an encrypted symmetric key via encrypting the symmetric key with a public key and decrypting the received encrypted symmetric key via a private key of the public key was well known in the art of secure key distribution. Such incorporation of key-encrypting-key techniques of Kaliski into the combination of Rofheart, Lundkvist, Kronenberg and Willey supplies these well-known utilities.

12. Claims 21, 31, 32 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, in view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1),

hereinafter referred to as Lundkvist, in further view of Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey.

<u>Re claim 21</u>: Rofheart teaches a first communication device (Fig 3, elts 302, 303 & 303N) configured for determining whether protected content stored on the first communication device are to be accessed by a second communication device (Fig 3, elt 301), the first communication device comprising:

means for [¶103] performing a round trip time measurement between the first communication device and the second communication device (Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134),

means for [¶103] checking whether the measured round trip time is within a predefined interval (Fig 6, elts 603 & 605; ¶117-¶118; Fig 8, elts 803, 805 & 807; ¶136; *Rofheart teaches determining the distance between two devices falls within the set of authentication criteria, e.g. D<r, r1<D<R2 or D=R; the distance D is calculated via the formula D = C* × Trt/2; *ergo, to satisfy the authentication criteria, one of the following must validate successfully: Trt < 2×r/C, 2*×r1/C < Trt < 2×R2/C or Trt = 2×R/C), and

wherein the round trip time measurement is an authenticated round trip time measurement (Fig 6, elts 605 – satisfied → 609 → 611; ¶118; ¶122; Fig 8, elts 807 – satisfied → 811 → 813 → 815; ¶135-¶136; ¶138).

However, Rofheart does not expressly disclose, yet,

Lundkvist teaches:

a memory storing a common secret [*O_RND; E_RND*] (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50), which is also stored on the second communication device, said common secret is used for generating signals used in performing the round trip time measurement in order to authenticate the round trip time measurement (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

However, the combination of Rofheart and Lundkvist does not expressly disclose, yet,

Willey teaches:

means for [Fig 6, elts 100 & 300] performing an authentication of the second communication device, the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules (Fig 5a, elt 6; ¶48-¶49); and

means for [Fig 6, elts 100 & 300] sharing the common secret with the second communication device if the second communication device is compliant (Fig 5a, elts 6—Yes→7; ¶48-¶49).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart and Lundkvist with the teachings of Willey, for the purpose of mutually authenticating the communicating the devices before sharing confidential data to prevent unauthorized snooping or linking of devices.

Re claim 31: The combination of Rofheart, Lundkvist and Willey teaches means for [¶103] transmitting a first signal from the first communication device to the second communication device at a first time t1, means for [¶103] receiving a second signal at a second time t2, means for determining a time difference between the first time t1 and the second time t2 (Rofheart: Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134).

The combination further teaches said second signal [Lundkvist: Fig 2, elt Y1; Fig 3, elts Z & Y2; Fig 4, elt Y3; Fig 5, elt Y4] according being generated according to the common secret [Lundkvist: *O_RND; E_RND*], means for [Fig 1, elts 1 & 2] checking if the second signal has been generated according to the common secret (Lundkvist: Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of

messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

Re claim 32: Rofheart teaches a first communication device configured for determining whether protected content stored on a first communication device are to be accessed by a second communication device, the second device being adapted for receiving a first signal from the first device, generating a second signal by modifying the received first signal according to a common secret, and transmitting the second signal to the first device, the first device comprising:

a transmitter (Figs 1 & 2);

a receiver (Figs 1 & 2);

a memory (Fig 2; ¶83-¶91); a bus connected to the memory (Fig 2; ¶83-¶91);

a processor connected to the bus and controlling the transmitter and receiver (Fig 1; Fig 2; ¶83-¶91), the processor executing the steps of:

measuring a round trip time between the first and the second communication device and checking whether said measured round trip time is within a predefined interval, the round trip time measurement being an authenticated round trip time measurement (Fig 6, elts 603 & 605; ¶117-¶118; Fig 8, elts 803, 805 & 807; ¶136; *Rofheart teaches determining the distance between two devices falls within the set of authentication criteria, e.g.* $D<r$, $r1<D<R2$ *or* $D=R$*; the distance D is calculated via the formula* $D = C \times Trt/2$; *ergo, to satisfy the authentication criteria, one of the following must validate successfully:* $Trt < 2 \times r/C$, $2 \times r1/C < Trt < 2 \times R2/C$ or $Trt = 2 \times R/C$), authenticating the second device, the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules (Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*).

However, Rofheart does not expressly disclose, yet,

Lundkvist teaches a memory storing a common secret [*O_RND; E_RND*] also stored on the second communication device (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50); said authenticated round trip time being determined based on said second signal generated according to the common secret (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

However, the combination of Rofheart and Lundkvist does not expressly disclose, yet, Willey teaches: transmitting the common secret to the second device after the second device has been authenticated (Fig 5a, elts 6—Yes→7; ¶48-¶49).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart and Lundkvist with the teachings of Willey, for the purpose of mutually authenticating the communicating the devices before sharing confidential data to prevent unauthorized snooping or linking of devices.

Re claim 34: The combination of Rofheart, Lundkvist and Willey teaches the processor performs the round trip measurement by: transmitting a first signal from the first device to the second device at time t1, and receiving a second signal from the second device at time t2, and determining a time difference between the first time t1 and the second time t2 (Rofheart: Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134).

The combination further teaches checking that the second signal [Lundkvist: Fig 2, elt Y1; Fig 3, elts Z & Y2; Fig 4, elt Y3; Fig 5, elt Y4] has been generated according to the common secret [Lundkvist: *O_RND; E_RND*] (Lundkvist: Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of

messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

13. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, in view of Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, and Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in further view of Traw et al (U.S. Pat 5949877 A), hereinafter referred to as Traw.

Re claim 22: Rofheart teaches a system for secure transfer of protected content comprising a first communication device in communication with a second communication device, the first communication device (Fig 3, elts 302, 303 & 303N) comprising:

processing means for [Fig 3, ¶102-¶103]:

performing a round trip time measurement between the first communication device and the second communication device (Fig 4, elt 403; ¶106; ¶108; Fig 7, all elements; ¶127-¶134), and

checking whether the measured round trip time is within a predefined interval, and wherein the round trip time measurement is an authenticated round trip time measurement, the authenticated round trip time measurement being performed using a signal that is generated and transmitted between the first and second devices (Fig 6, elts 603 & 605; ¶117-¶118; Fig 8, elts 803, 805 & 807; ¶136; *Rofheart teaches determining the distance between two devices falls within the set of authentication* *criteria, e.g. D<r, r1<D<R2 or D=R; the distance D is calculated via the formula D = C ×* Trt/2; *ergo, to satisfy the authentication criteria, one of the following must validate successfully: Trt < 2×r/C, 2*×r1/C < Trt < 2×R2/C or Trt = 2×R/C);

performing an authentication of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device (Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*); the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules (Fig 8, elt 801; ¶135; *the claimed set of predefined compliance rules can comprise a single rule; Rofheart teaches determining whether the unique identifier of the communicating device is on an ID list and determines whether or not said identifier is on the list which teaches the claimed set of predefined compliance rules*),

transmitting the protected content to the second device depending on the authenticated round trip time measurement being within the predefined interval (Fig 6, elts 605 – satisfied → 609 → 611; ¶118; ¶122; Fig 8, elts 807 – satisfied → 811 → 813 → 815; ¶135-¶136; ¶138).

However, Rofheart does not expressly disclose, yet,

Lundkvist teaches

a memory for storing a common secret [*O_RND; E_RND*] (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50),

the authenticated round trip time measurement being performed using a signal that is generated using the common secret (Fig 2, all elements; ¶31-¶32; Fig 3, all elements; ¶33-¶34; Fig 4, all elements; ¶36-¶38; ¶44-¶49; Fig 5, all elements; ¶50).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart with the teachings of Lundkvist, for the purpose of not only authenticating the distance between two devices, as is taught by both Rofheart and Lundkvist, but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

However, Rofheart and Lundkvist does not expressly disclose, yet,

Willey teaches securely sharing the common secret with the second communication device if the second communication device is compliant (Fig 5a, elts 6—Yes→7; ¶48-¶49).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart and Lundkvist with the teachings of Willey, for the purpose of mutually authenticating the communicating the devices before sharing confidential data to prevent unauthorized snooping or linking of devices.

However, the combination of Rofheart, Lundkvist and Willey does not expressly disclose, yet,

Traw teaches said identification being based on a certificate in the second device (Fig 1a, elt 112; Fig 1b, elt 116; Fig 1c, elt 130 & 134; col 6, lines 25-35; col 7, lines 5-65).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist and Willey with the teachings of Traw, for the purpose of validating compliancy of each device and cryptographically tying the device identification information to the device itself via a digital certificate, as is taught by Traw.

14. Claims 30 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rofheart et al (U.S. Pat App Pub 2005/0265503 A1), hereinafter referred to as Rofheart, Lundkvist (U.S. Pat App Pub 2003/0184431 A1), hereinafter referred to as Lundkvist, and Willey (U.S. Pat App Pub 2003/0065918 A1), hereinafter referred to as Willey, in further view of Kaliski, Jr. (U.S. Pat 6085320 A), hereinafter referred to as Kaliski.

<u>Re claims 30 and 33</u>: The combination of Rofheart, Lundkvist and Willey teaches all the limitations of claims 21 and 32 as previously stated.

Kaliski teaches means arranged to [Fig 1; Fig 4A, elts 20 & 40] securely share the common secret [Figs 3A & 3B: elt *session key KSS*] with the second device by encrypting the common secret [Figs 3A & 3B: elt *session key KSS*] using a public key

[Figs 3A & 3B: elt *PUB*$_{SERV}$] of a private/public key-pair [Figs 3A & 3B: elts *PUB*$_{SERV}$ *and PRIV*$_{SERV}$] (Figs 3A & 3B; col 4, line 32 – col 5, line 29).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Rofheart, Lundkvist and Willey with the teachings of Kaliski, for the purpose of protecting the symmetric key from unauthorized exposure; using key-encrypting-key techniques, specifically transmitting an encrypted symmetric key via encrypting the symmetric key with a public key and decrypting the received encrypted symmetric key via a private key of the public key was well known in the art of secure key distribution. Such incorporation of key-encrypting-key techniques of Kaliski into the combination of Rofheart, Lundkvist and Willey supplies these well-known utilities.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29

USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 14, 15 and 17-34 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 3, 5-11 and 13 of copending Application No. 10/521858.

This is a provisional obviousness-type double patenting rejection.

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Darren B. Schwartz whose telephone number is (571)270-3850. The examiner can normally be reached on 7am-5pm EST, Monday-Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Darren B Schwartz/
Primary Examiner, Art Unit 2435

34

REPLY UNDER 37 CRF 1.116
EXPEDITED PROCEDURE
TECHNOLOGY 2435

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Kamperman, Frank.	Attn. No.: 2002P02007 US
SERIAL NO.: 12/508,917	EXAMINER: Schwartz, D.B.
FILED: 07/24/2009	ART UNIT: 2435
	CONFIRMATION No.: 8927

TITLE: SECURE AUTHENTICATED DISTANCE MEASUREMENT

Mail Stop: AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AFTER FINAL OFFICE ACTION

Dear Sir:

In response to the Office Action dated January 4, 2013, applicant submits this paper within two (2) months **(until March 4, 2013)** of the mailing date of the Office Action and requests amendment of the above identified application wherein:
Amendments made to the claims begin on page 2; and
Remarks begin on page 9.

As this paper is being filed within two (2) months of the mailing date of the instant Office Action, applicant respectfully requests that the entry of this paper into the record be expedited to allow the Examiner sufficient time to review the arguments presented herein within the statutory time period.

IN THE CLAIMS:

Kindly replace the claims of record with the following full set of claims:

1. – 13. (Cancelled)

14. (Currently amended) A method of determining whether protected content stored on a first communication device ~~(201, 301)~~ are ~~to be~~ accessed by a second communication device ~~(203, 303)~~, the method comprising the step of:

performing ~~(209)~~ a round trip time measurement between the first communication device and the second communication device,

checking whether the round trip time is within a predefined interval, and

allowing access of the protected content provided that the round trip time is within the predefined interval, ~~wherein the round trip time measurement is an authenticated round trip time measurement, and~~ wherein the first and the second communication device share a common secret, and said common secret is used for generating signals used in performing the round trip time measurement ~~in order to authenticate the round trip time measurement~~ between the first and second communication device, said signals used in performing the round trip time measurement being generated in each of said first device and said second device using a similar process,

and wherein:

the first device ~~(201, 301)~~ authenticates the second device (203, 303), the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules, and

the first device ~~(201, 301)~~ securely shares the common secret with the second device (203, 303) according to a key management protocol after having authenticated the second device.

15. (Currently amended) The method according to claim 14, wherein the ~~authenticated~~ round trip time measurement comprises the steps of:

transmitting ~~(305)~~ a first signal from the first communication device ~~(201, 301)~~ to the second communication device ~~(203, 303)~~ at a first time t1, the second communication device being adapted for receiving ~~(311)~~ the first signal;

generating ~~(313)~~ a second signal according to the common secret, and transmitting ~~(315)~~ the second signal to the first device;

receiving ~~(317)~~ the second signal at a second time t2;

checking ~~(319)~~ if the second signal has been generated according to the common secret; and

determining ~~(323)~~ a time difference between the first time t1 and the second time t2.

16. (Cancelled)

17. (Currently amended) The method according to claim 15, wherein the step of checking ~~(319)~~ if the second signal has been generated according to the common secret comprises the steps of:

generating a third signal according to the common secret; and

comparing the third signal with the received second signal.

18. (Currently amended) The method according to claim 15, wherein the first signal and the common secret are bit words and where the second signal comprises modifying the first signal ~~information being generated~~ by performing an XOR of the first signal with the common secret ~~between the bit words~~.

19. (Currently amended) The method according to claim 14, wherein the authentication check ~~(205)~~ of the second device further comprises the step of checking if the identification of the second device is compliant with an expected identification.

20. (Previously presented) The method according to claim 14, in which the key management protocol comprises one of a key transport protocol and a key agreement protocol.

21. (Currently amended) A first communication device ~~(201, 301, 406)~~ configured for determining whether protected content stored on the first communication device ~~are to be~~ is accessed by a second communication device ~~(203, 303)~~, the first communication device comprising:

~~means for performing a round trip time measurement between the first communication device (201) and the second communication device (203),~~

~~means for checking whether the measured round trip time is within a predefined interval, and wherein the round trip time measurement is an authenticated round trip time measurement,~~

~~a memory storing a common secret, which is also stored on the second communication device, said common secret is used for generating signals used in performing the round trip time measurement in order to authenticate the round trip time measurement:~~

means for performing ~~(205)~~ an authentication of the second communication device, the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules; ~~and~~

means for securely sharing a common secret with the second communication device after the second communication device is determined to be compliant with the predefined compliance rules;

means for performing a round trip time measurement between the first communication device and the second communication device, wherein said common secret is used in a similar process by each of said first device and said second device for generating signals used in performing the round trip time measurement;

means for checking whether said signals generated by said first device and said second device are identical;

means for checking whether the measured round trip time is within a predefined interval when said signals generated by said first device and said second device are determined to be identical, and

means for allowing access to said protected content when said measured round trip time is within the predefined interval.

22. (Currently amended) A system for secure transfer of protected content comprising a first communication device ~~(201, 301, 406)~~ in communication with a second communication device ~~(203, 303),~~ the first communication device comprising:

a memory ~~for~~ storing a common secret,

processing means ~~for~~:

performing an authentication of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device;

securely sharing the common secret with the second communication device if the second communication device is compliant with the expected identification;

performing a round trip time measurement between the first communication device and the second communication device, wherein signals used in said round trip time measurement are generated using the common secret in a same process in each of said first and second communication devices, ~~and~~

checking whether the measured round trip time is within a predefined interval, ~~and wherein the round trip time measurement is an authenticated round trip time measurement, the authenticated round trip time measurement being performed by using a signal that is generated using the common secret and transmitted between the first and second devices,~~

~~performing (205) an authentication of the second communication device by checking whether the second communication device is compliant with an expected identification of the second communication device, said identification being based on a certificate in the second device; the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules~~,

~~securely sharing (207) the common secret with the second communication device if the second communication device is compliant~~; and

transmitting the protected content to the second device depending on the ~~authenticated~~ round trip time measurement is ~~being~~ within the predefined interval.

23. (Previously presented) The method according to claim 14, wherein the common secret is securely shared with the second device by encrypting the common secret using a public key of a private/public key-pair.

24. (Cancelled)

25. (Previously presented) The method according to claim 14, wherein the protected content stored on the first device ~~(201)~~ is sent to the second device ~~(203)~~ if it is determined that the protected content stored on the first device ~~(201)~~ is permitted to be shared with the second device ~~(203)~~.

26. (Cancelled)

27. (Cancelled)

28. (Currently amended) The method according to claim 14, wherein securely sharing the common secret with the second device ~~(203)~~ by the first device ~~(201)~~ comprises transmitting a random generated bit word to the second device ~~(203)~~.

29. (Currently amended) The method according to claim 14, wherein the shared common secret is used for generating a secure authenticated channel between the first ~~(201)~~ and the second communication device~~ (203)~~.

30. (Currently amended) The first communication device ~~(201)~~ according to claim 21, further comprising

means arranged to securely share the common secret with the second device (203) by encrypting the common secret using a public key of a private/public key-pair.

31. (Currently amended) The first communication device ~~(201)~~ according to claim 21, further comprising:

means for transmitting ~~(305)~~ a first signal from the first communication device (201) to the second communication device ~~(203)~~ at a first time t1,

means for receiving ~~(317)~~ a second signal at a second time t2, said second signal being generated by modifying the first signal according to the common secret,

means for checking (319) if the second signal has been generated according to the common secret, said checking comprising:

generating a third signal by modifying the first signal according to the common secret; and

comparing the third signal with the second signal,

means for determining ~~(323)~~ a time difference between the first time t1 and the second time t2.

32. (Currently amended) A first communication device ~~(201)~~ configured for determining whether protected content stored on a first communication device ~~(201)~~ is ~~to be~~ accessed by a second communication device (203), the second device ~~(203)~~ being adapted for receiving ~~(311)~~ a first signal from the first device, generating ~~(313)~~ a second signal by modifying the received first signal according to a common secret, and transmitting ~~(315)~~ the second signal to the first device, the first device comprising:

a transmitter ~~(411)~~;

a receiver ~~(403)~~;

a memory ~~(305)~~ storing a common secret ~~also stored on the second communication device~~;

a bus ~~(417)~~ connected to the memory;

a processor ~~(413)~~ connected to the bus and controlling the transmitter and receiver, the processor executing the steps of:

measuring a round trip time between the first ~~(201)~~ device and the second ~~communication~~ device, said measured round trip time being determined based on a time difference between signals transmitted between the first and second devices, wherein the signals used in said round trip measurement are generated using the common secret in a same process in each of the first device and second device; ~~(203) and~~

checking whether said measured round trip time is within a predefined interval~~, the round trip time measurement being an authenticated round trip time measurement, said authenticated round trip time being determined based on said second signal generated according to the common secret, and~~

authenticating the second device (203), the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules; and

securely transmitting the common secret to the second device after the second device has been authenticated.

33. (Currently amended) The first communication device ~~(201)~~ of claim 32 wherein the processor securely shares the common secret with the second communication device by encrypting the common secret using a public key of a private/public key-pair.

34. (Currently amended) The first communication device ~~(201)~~ of claim 32 wherein the processor performs the round trip time measurement by:

transmitting a first signal from the first device to the second device at time t1, ~~and~~

receiving a second signal from the second device at time t2,

modifying the first signal by the common secret;

~~checking~~ determining that the second signal ~~has been generated~~ and the first signal modified according to the common secret are identical, and

determining a time difference between the first time t1 and the second time t2.

REMARKS

Entry of this Amendment and reconsideration are respectfully requested in view of the above amendments and the following remarks.

Claims 14-15 and 17-34 are pending and stand rejected.

Claims 14, 21, 22 and 32 are independent claims.

Claims 14, 15, 17, 18, 19, 21, 22, 25, 28, 29, 30, 31, 32, 33 and 34 have been amended. Claims 24, 26, and 27 have been cancelled without prejudice.

Claims 14, 15, 19, 20 and 24-29 stand rejected under 35 USC 103(a) as being unpatentable over Rofheart (US 2005/0265503) and Lundkvist IUS 2003/0184431) and further in view of Kronenberg (US 2002/078227) and Willey (US 2003/0065918). Claims 17 and 18 stand rejected under 35 USC103 (a) over Rofheart, Lundkvist, Kronenberg and Willey and further in view of Caputo (US 5,778,071). Claim 23 stands rejected under 35 USC 103(a) as being unpatentable over Rofheart, Lundkvist, Kronenberg and Willey and further in view of Kaliski (US 6085320). Claims 21, 31, 32 and 34 stand rejected under 35 USC 103(a) as being unpatentable over Rofheart, Lundkvist, and Willey (US 2003/0065918). Claim 22 stands rejected under 35 USC 103(a) as being unpatentable over Rofheart, Lundkvist, Willey and Traw (US 5,949,877). Claims 30 and 33 stand rejected under 35 USC 103(a) as being unpatentable over Rofheart, Lundkvist, and Willey and further in view of Kaliski.

Claims 14, 15 and 17-34 are provisionally rejected on the ground of non-statutory obviousness-type double patenting over claims 1, 3, 5-11 and 13 of co-pending application no. 10/521,858.

With regard to the rejection of claims 14, 15 and 17-34 as being provisionally rejected based on the statutory obviousness-type double patenting over the claims of co-pending application, serial no. 10/521,858, applicant continues to respectfully request that the rejection be held in abeyance until such time that either the instant application issues or the co-pending application issues and the issued claims may be examined to determine whether the rejection is still applicable.

In supporting the rejection of claims 14, 15, 19, 20 and 24-29 as being unpatentable over Rofheart, Lundkvist, Kronenberg and Willey, the Office Action asserts, with regard to claim 14, that **Rofheart** teaches a method of determining whether protected content stored on a first communication are to be accessed by a second communication device, the method comprising: performing a round trip time measurement between the first communication device and he second communication device, checking whether the round trip time is within a predefined interval I (Rofheart teaches determining the distance between two devices falls within the set of authentication criteria e.g., D<r, r1<D<R2 or D=R, the distance D is calculated via the formula D=CxTrt/2, therefore to satisfy the authentication criteria, one of the following must validate successfully: Trt >2xr/C, 2xr1/C<Trt<2xR2/C or Trt = 2xR/C), allowing access of the protected content provide that the round trip time is within the predefined interval, where the round trip time measurement is an authenticated round tip time measurement, the first device authenticates the second device, the authentication of the second device includes verifying that the second device complies with a set of predefined compliance rules (Fig. 8, 801, para. 0135, the claimed set of predefined compliance rules can comprise a single rule).

The Office Action acknowledges that Rofheart does not expressly disclose yet **Lundkvist** teaches, wherein the first and the second communication device share a common secret (Fig. 2, para. 0031, 0032, Fig. 3, Fig. 4, Fig. 5).

The Office Action asserts that it would have been obvious to modify the teachings of Rofheart from the teachings of Lundkvist for the purpose of not only authenticating the distance between two devices but also protecting the actual exchange of messages between the devices to inhibit unauthorized access to the communicating messages themselves which reduces risks associated with tampering.

The Office Action further acknowledges that the combination of Rofheart and Lundkvist does not expressly disclose, yet **Kronenberg** teaches, the first device securely shares the common secret with the second device according to a key management protocol. It would have been obvious to modify Rofheart and Lundkvist with the teachings of Kronenberg for the purpose of protecting both the confidentiality of exchanged information but also the authenticity of exchanged information for the known purpose of providing non-repudiation and resistance to tampering of such information.

The Office Action further states that Rofheart, Lundkvist and Kronenberg does not expressly disclose, yet **Willey** teaches, the first device securely shares the common secret with the second device after having authenticated the second device.

Applicant respectfully disagrees with and explicitly traverses the rejection of the claims.

Rofheart, as read by the applicant, teaches a system for determining a distance between a local device and a plurality of remote devices wherein a round trip time is determined as the difference between a time, t1, of transmitting a signal to a remote device and a time, t1, of receiving a return signal from the remote device considering a processing time, d, a the remote device. If the measured distance to the remote device, as determined by the measured round trip time, then Rofheart allows communication between the local device and the remote device.

Lundkvist discloses a system for controlling authorization for access to an object in which signal communication is established wherein a first signal is sent from an object to a portable device and at least one second signal is sent from the portable device to the object. The second signal represents an encryption of the first signal with additional information to verify that the portable device is an approved identity. Lundkvist further discloses that after the verification information is checked, a distance is measured between the object and the portable device. The measured distance is then checked against a distance measure. The measured distance is determined based on a time for the transmission of one of the first and second signals.

The system of Lundkvist, thus, teaches encryption of a first signal, which includes identification information of the portable device (O_ID) and a random number (O_RND). The portable device receives the encrypted signal and decrypts the encrypted signal to obtain the identification and the random number. The portable device then encrypts the first signal as E_SVAR+f(O_RND). ***The portable device transmits the encrypted signal back to the object, which decrypts*** the received signal to obtain the message portion (i.e., O_RND). When both the message portion and the time are validated, then an action may be performed by the object (e.g., unlock a car door).

Thus, Lundkvist teaches that the verification (authentication) and the distance measure are performed at the same time and that an encryption and decryption process are used to securely transmit the information between the two devices.

Assuming that the encryption of the first signal is performed using a common secret, Lundkvist teaches that both the object (i.e., local device of Rofheart) and the portable device (i.e. remote device of Rofheart) have the common secret that is used to encrypt the first signal and the identification.

Thus, ***Lundkvist teaches both devices have the common secret prior to authenticating the device is compliant with compliance rules and, thus, Lundkvist fails to disclose that the common secret is shared after the compliance of the portable device has been authenticated*** (i.e., claim element "*securely transmitting the common secret to the second device after the second device has been authenticated.*"

Kronenberg, as read by the applicant, teaches a system for storing secure information in a network by transmitting secure packets and non-secure packets throughout the network, wherein secure packets are received by secure relays and the secure packets are provided to different secure relays. The non-secure packets are sent from the receiving relay onto the destination relay.

The Office Action refers to para. 0009 of Kronenberg for teaching "the first device securely shares the common secret with the second device according to a key management protocol.

However, a reading of para. 0009 reveals that Kronenberg teaches "IPSec (IP Security) is a series [of[guidelines for the protection of Internet Protocol (IP) communications. It specifies ways for securing private information transmitted over public networks. Services supported by IPSec include confidentiality (encryption), authenticity (proof of sender) integrity (detectionof data tampering) and replay protection (defense against unauthorized re0sendign of data. IPSec also specifies methodologies for key management..."

Kronenberg, thus, discloses known security guide lines that provides for transmitting information securely over a network.

However, even if it could be said that Kronenberg transmits data securely over a network, Kronenberg is silent with regard to the claim element of "***securely transmitting the common secret to the second device after the second device has been authenticated.***"

That is, Kronenberg fails to disclose that the IPsec rules are implemented after the second deice has been authenticated (i.e., compliant with compliance rules).

Willey, as read by the applicant, teaches a system in which a link key may be established between two devices wherein one device is an authenticating device and the other is an authenticated device.

The Office Action asserts that Willey teaches "the first device securely shares the common secret with the second device after having authenticated the second device (figure 5a and para. 0048-0049).

However, with regard to Figure 5a, which is described starting at para. 0040, Willey discloses "[d]uring key agreement, in step 3, each device 100 or 300 exchanges public keys by sending a message that include its public key to the other device 100 or 300. The next step 4 *incudes the computation of the shared secret by both devices 100* *and 300 so that as a result of the key agreement procedure both devices 100 and 300 have a shared secret value that is used to derive a symmetric key 36. "*

Thus, Willey discloses that the common secret is developed by each device based on a key agreement procedure.

Willey fails to disclose securely sharing the common secret after the second device has been determined to be compliant.

Willey further discloses "the symmetric key or antispoof variable or [sic] is computed in device 100, 300 to ensure that both devices 100, 300 have the same secret key. *The antispoof variable is based upon a one way function of the shared secret.* ... In step 5, the handset 100 informs the user 400 via the display 160 that in order to complete the pairing procedure the user 400 should verify that each digit that is about to be displayed by the display 160 is the same as the digit to be announced simultaneously via the speaker 40. The devices 100 and 300 then begin the process of indicating the digits of the antispoof variable 36 to the user 400 one after another. The simultaneous display and announcement of the digits on either device 100, 300 substantially diminishes the threat of man-in-the middle attack." (see para. 0042-0043).

Paragraphs 0043-0047 disclose that process of verifying the digits of the antispoofing variable that are presented to the user.

In paragraph 48, Willey discloses that "[a]fter the user 400 has given positive confirmation of both the headset 300 and the handset 100, then the devices are fully authenticated. In the next step 7, the devices 100 and 300 securely establish the link key. For example, the devices 100, 300 can both derive a symmetric encryption key based upon the elliptic curve D-H shared secret. A link key is created and encrypted using the encryption key and sent to the other device 300 which decrypts and stores it."

Thus, Willey teaches each device develops a secret key that is used to generate a symmetric key 36. The symmetric key is then used to authenticate the devices in that each device has produced the same symmetric key. After authentication, then a link key is established in one device and then sent to the second device. Alternatively, a PIN may be sent from one device to another by encrypting the PIN and the second device then the two devices would establish a link key based on the shared PIN.

Assuming that the authentication is comparable to the preset compliance rules, then, accordingly, the link key or the PIN would be comparable to the common secret.

However, the link key or the PIN is not comparable to the common secret recited in the claims, as neither the link key nor the PIN provide for generating signals that are used in the distance measurement. Rather the PIN is used by each device to generate a link key and the link key is used to encrypt data that is transmitted over the link.

Thus, even if the teachings of cited references were combined, the combination would not teach the element of "securely sharing the common secret ... if the second device is compliant.' (see claim 21). Similar elements are recited in the other independent claims. (e.g., claim 14, "securely sharing ... the common secret...,"claim 22, "securely sharing the common secret...", and claim 32, "securely transmitting the common secret...").

Notwithstanding the arguments presented above, the independent claims have been further amended to recite "wherein the first and the second communication device share a common secret, and said common secret is used for generating signals, in each of said first device and said second device using the common secret in a similar process, used in performing the round trip time measurement." No new matter has been added. Support for the amendment may be found on at least page 8, lined 25-32," The second device receives the signal via a receiver 311 and 313 modifies the signal by using the locally stored secret. The signal is modified according to rules known by the first device 301 and transmitted back to the first device 301 via a transmitter 315. The first device 301 receives the modified signal via a receiver 317 and in 319 the received modified signal is compared to a signal, which has been modified locally. The local modification is performed in 321 by using the signal transmitted to the second device in 309 and then modifying the signal using the locally stored secret similar to the modification rules used by the second device."

None of the references teaches that the signals used in the distance measurement are signals that are generated in each of the first and second device using the common secret in a same process.

Rather each of the references essentially teaches that a first signal may be sent to a second device, in which the second device may then encrypt the received first signal, using a link key or a long PIN, for example, and the encrypted second signal is then provided back to the first device. The first device may then decrypt the received encrypted message.

For example, the combination of the cited references may disclose that a link key or PIN (from which a link key may be generated) may be exchanged and the link key may be used to encrypt a signal that may be used in the distance measurement. The second device performs an encryption process to modify the signal and the first device performs a decryption process (i.e., two different processes) to obtain the original signal, which determines whether the two signals are identical.

Thus, the first and second devices use different processes to generate signals that are used in the distance measurement. That is, the second device encrypts the signal and the first device receives the encrypted signal and decrypts the received encrypted signal to determine whether the signal has been processed in accordance with the common secret.

With regard to the assertion that it would be obvious to amend Rofheart to incorporate the teachings of Lundkvist, Kronenberg and Willey, Applicant would note that in addressing obviousness determination under 35 USC 103, the 'Supreme Court in *KSR International Co. v. Teleflex Inc.*, (citation omitted) reaffirmed many of its precedents relating to obviousness including its holding in *Graham v. John Deere Co. (citation omitted)*. In particular e Court in *KSR International v. Teleflex Inc.* (citation omitted) addressed the standard for obviousness that had been imposed in decisions rendered by the CAFC in that there must be some teaching, suggestion or motivation (TSM) to combine the known elements in the same manner set forth in the claims and found that the TSM to combine provides a "helpful hint" in determining whether claimed subject matter is obvious. The Court however stated that the application of the TSM (teaching, suggestion, motivation) test is not to be applied in a rigid manner and a bright light application of such a test is adverse to those factors for determining obviousness enumerated in the _Graham v. John Deere_ (i.e., the scope and content of the prior art, the level of ordinary skill in the art, the differences between the claimed invention and the prior art and objective indicia of non-obviousness) (citation omitted).

In _KSR,_ the Court also reaffirmed that "a patent composed of several elements is not obvious merely by demonstrating that each of its elements was, independently, known in the prior art." In this regard, the KSR court stated that "it can be important to identify a reason that would have prompted a person of ordinary skill in the ... field to combine the elements in the way the claimed new invention does ... because inventions in most, if not all, instances rely upon building blocks long since uncovered and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known."

Furthermore, the Court in _KSR_ did not diminish the requirement for objective evidence of obviousness ("[r]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). When prior art references require a selected combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight gained from the invention. i.e., something in the prior art as a whole must suggest the desirability and thus the obviousness of making the combination. _Uniroyal Inc. V. Rudlkin-Wiley Corp_ (citation omitted).

In this case, none of the references provides any teaching regarding "wherein the first and the second communication device share a common secret, and said common secret is used for generating signals***, in each of said first device and said second device using the common secret in a similar process,*** used in performing the round trip time measurement" or " "***transmitting the common secret to the second device after the second device has been authenticated***."

Thus, even if the teachings of Willey, Kronenberg and Lundkvist were combined with the teachings of Rofheart, the combination would fail to teach or suggest all the recited claim elements.

Accordingly, the combination of the cited fails to render unpatentable the subject matter recited in the independent claim 14 and the claims. 15, 19, 20 and 24-29, which depend from claim 14.

With regard to the rejection of claims 21, 31, 32 and 34, of which claims 21 and 32 are independent claims, as being unpatentable over Rofheart and Lundkvist and further in view of Kronenberg and Willey, applicant respectfully disagrees with and explicitly traverses the rejection of the claims.

Independent claims 21 and 32 recite subject matter similar to that recited in claim 14 and have been amended in a similar manner.

Hence, the arguments presented above with regard to independent claim 14 are also applicable in response to the rejection of claims 21 and 32.

Accordingly, for the same arguments presented with regard to claim 14, which are repeated, as if in full, with regard to claims 21 and 32, applicant submits that the reason for the rejection of the claims has been overcome.

With regard to the rejection of independent claim 22 as being unpatentable over Rofheart, Lundkvist, Willey and Traw, applicant respectfully disagrees with and explicitly traverses the rejection of the claim.

Independent claim 22 recites subject matter similar to that recited in claim 14 and has been amended in a similar manner.

Hence, the arguments presented above with regard to independent claim 14 are also applicable in response to the rejection of claim 22.

Accordingly, for the same arguments presented above, which are repeated, as if in full, with regard to claim 22, applicant submits that the reason for the rejection of the claims has been overcome.

With regard to the rejection of the remaining claims, these claims depend from corresponding ones of the independent claims and inherit subject matter from the independent claims from which they depend, and which has been shown not to be disclosed by the cited references. Accordingly, the remaining claims are also not rendered unpatentable over the cited references as the remaining claims include subject matter that is not disclosed by the primary prior art references and any of the other prior art references.

With regard to the rejection of the claims under the judicially created doctrine of double patenting, applicant respectfully requests that this rejection be held in abeyance until such time that this application or the referred to application issues and the claims in the current application may be compared to the issued claims to determine if the rejection is still applicable.

For the amendments made to the claims and for the remarks made herein, applicant submits that the reasons for the rejection of the claims have been overcome.

Applicant respectfully requests that that the rejections of the claims be withdrawn and a Notice of Allowance be issued.

Applicant denies any statement, position or averment stated in the Office Action that is not specifically addressed by the foregoing. Any rejection and/or points of argument not addressed are moot in view of the presented arguments and no arguments are waived and none of the statements and/or assertions made in the Office Action is conceded.

Applicant makes no statement regarding the patentability of the subject matter recited in the claims prior to this Amendment and has amended the claims solely to facilitate expeditious prosecution of this patent application. Applicant respectfully reserves the right to pursue claims, including the subject matter encompassed by the originally filed claims, as presented prior to this Amendment, and any additional claims in one or more continuing applications during the pendency of the instant application.

In order to advance the prosecution of the matter, applicant respectively requests that any errors in form that do not alter the substantive nature of the arguments presented herein be transmitted telephonically to the applicant's representative so that such errors may be quickly resolved or pursuant to MPEP 714.03 be entered into the record to avoid continued delay of the prosecution of this matter any further.

MPEP 714.03 affords the Examiner the discretion, pursuant to 37 CFR 1.135 (c), to enter into the record a bona fide attempt to advance the application that includes minor errors in form.

"[a]n Examiner may treat an amendment not fully responsive to a non-final Office Action by: (A) accepting the amendment as an adequate reply to the non-final Office action to avoid abandonment ... (B) notifying the applicant that the reply must be completed... (C) setting a new time period for applicant to complete the reply ...

The treatment to be given to the amendment depends upon:

(A) whether the amendment is bona fide; (B) whether there is sufficient time for applicant's reply ... (C) the nature of the deficiency.

Where an amendment substantially responds to the rejections, objections or requirements in a non-final Office action (and is bona fide attempt to advance the application to final action) but contains a minor deficiency (e.g., fails to treat every rejection, objection or requirement), the examiner may simply act on the amendment and issue a new (non-final or final) Office action. The new Office action may simply reiterate the rejection, objection or requirement not addressed by the amendment (or otherwise indicate that such rejection, objection or requirement is no longer applicable).

This course of action would not be appropriate in instances in which an amendment contains a serious deficiency (e.g., the amendment is unsigned or does not appear to have been filed in reply to the non-final Office action)..."

However, if the Examiner believes that such minor errors in form cannot be entered into the record or that the disposition of any issues arising from this response may be best resolved by a telephone call, then the Examiner is invited to contact applicant's representative at the telephone number listed below to resolve such minor errors or issues.

No fees are believed necessary for filing this paper.

Respectfully submitted,

Date: February 28, 2013 /Carl A. Giordano/

By: Carl A. Giordano
Attorney for Applicant
Registration No. 41,780
(914) 391 8104

Mail all correspondence to:
Michael E. Belk, Esq.
US PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9643
Fax: (914) 332-0615

35

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/508,917	07/24/2009	Franciscus Lucas Antonius Johannes KAMPERMAN	2002P02007 US	8927

24737 7590 03/11/2013
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
03/11/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

debbie.henn@philips.com
marianne.fox@philips.com

PTOL-90A (Rev. 04/07)

Advisory Action **Before the Filing of an Appeal Brief**	**Application No.** *12/508,917*	**Applicant(s)** KAMPERMAN, FRANCISCUS LUCAS ANTONIUS JO
	Examiner Darren B. Schwartz	**Art Unit** 2435

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 01 March 2013 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:

a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.

b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because

a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);

b) ☐ They raise the issue of new matter (see NOTE below);

c) ☒ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☒ will not be entered, or (b) ☐ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.

12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

13. ☐ Other: _____.

STATUS OF CLAIMS

14. The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: .
Claim(s) objected to: .
Claim(s) rejected: 14,15 and 17-34.
Claim(s) withdrawn from consideration: .

/Darren B Schwartz/
Primary Examiner, Art Unit 2435

U.S. Patent and Trademark Office

Continuation of 11. does NOT place the application in condition for allowance because: The amendments to the claims alter the scope of the claims necessitating further search and consideration of the art. It is also noted that the claims, as filed 01 March 2013, of which are not entered, provisionally raise issues under 35 U.S.C. 112(2)/112(B) as it is unclear as to the metes and bounds of "a similar process" as per amended independent claims 14, 21 22 & 32. It is unclear as to how a process in said first device is "similar" to a process in said second device as generally claimed; more to the point, it is unclear as to the standard of measure as what qualifies as "similar". It is noted that processes are The arguments filed 01 March 2013 have been carefully considered but are not persuasive. The following precedence has been held: NTP, Inc. v. Research in Motion, Ltd., 418 F.3d 1282, 1316 (Fed. Cir. 2005) ("A process is a series of acts." (quoting Minton v. Nat'l Ass'n of Sec. Dealers, Inc., 336 F.3d 1373, 1378 (Fed. Cir. 2005))); In re Kollar, 286 F.3d 1326, 1332 (Fed. Cir. 2002) ("[A] process . . . consists of a series of acts or steps . . . . It consists of doing something, and therefore has to be carried out or performed."). To claim a process a process is similar to another process does not establish a measure by which to determine similarity as to the series of acts that make up that process.

On page 12 of Remarks, Applicant addresses the teachings of Rofheart.

The Examiner in no way concedes nor subscribes to Applicant's summarization or distillation of the art of record; it is further noted that Applicant does not address any apparent section, paragraph or column of the Rofheart.

On page 12 of Remarks, Applicant addresses the teachings of Lundkvist.

The Examiner in no way concedes nor subscribes to Applicant's summarization or distillation of the art of record; it is further noted that Applicant does not address any apparent section, paragraph or column of the Lundkvist.

On page 13 of Remarks, Applicant argues: "Thus, Lundkvist teaches both devices have the common secret prior to authenticating the device is compliant with compliance rules and, thus, Lundkvist fails to disclose that the common secret is shared after the compliance of the portable device has been authenticated (i.e. claim element 'securely transmitting the common secret to the second device after the second device has been authenticated.'"

This argument is unpersuasive as the Examiner never applies the Lundkvist reference as teaching the claimed the device is compliant with compliance rules. The only references applied as teaching the claimed are as follows: Rofheart was applied as teaching the claimed complaint with an expected identification and verifying that the second device complies with a set of predefined compliance rules, Willey was applied as teaching the claimed sharing the common secret with the second communication device if the second communication device is compliant. Applicant is not addressing the Examiner's actual positions.

On pages 13 & 14 of Remarks, Applicant addresses the teachings of Kronenberg.

The Examiner in no way concedes nor subscribes to Applicant's summarization or distillation of the art of record; it is further noted that Applicant does not address any apparent section, paragraph or column of the Kronenberg.

Applicant's arguments as per the Kronenberg reference are unpersuasive as Kronenberg is not applied as teaching the claim element of 'securely transmitting the common secret to the second device after the second device has been authenticated' but it, in fact, applied as teaching the first device securely shares the common secret with the second device <<<according to a key management protocol>>>. Applicant is not addressing the Examiner's actual position.

On page 14 of Remarks, Applicant addresses the teachings of Willey, stating "However, with regard to Figure 5a, which is described starting at para. 0040[.]"

While paragraph 40 addresses Figure 5a of Willey, it does not form the basis of the Examiner's position and so Applicant is not addressing the Examiner's actual position.

On page 15 of Remarks, Applicant argues: "Thus, WIley teaches each device develops a secret key that is used to generate a symmetric key 36. The symmetric key is then used to authenticate the devices in that each device has produced the same symmetric key. After authentication, then a link key is established in one device and then sent to the second device. Alternatively, a PIN may be sent from one device to another by encrypting the PIN and the second device then the two devices would establish a link key based on the shared PIN."

Applicant appears to be summarizing the teachings of the Willey reference; the Examiner's position is explicit in addressing Figure 5a, elts 6 & 7 (see Final Rejection). Applicant is not addressing the Examiner's actual position.

On page 16 of remarks, Applicant indicates "Support for the amendment may be found on at least page 8, lines 25-32[.]"

Such citations further raise the issues of new matter and indefiniteness as while there is explicit support for the locally stored secret "similar" to the modification rules used by the second device, there is no expressed nor inherent support for a similar "process" or a similar "process".

On page 17 of remarks, Applicant argues: "None of the references teaches that the signals used in the distance measurement are signals that are generated in each of the first and second device using the common secret in a same process."

Aside from the potential issues of new matter and potential issues of indefiniteness, as best understood, the Examiner disagrees as the combined teachings of the references are applicable to such limitation. For instance, without limitation nor disclaimer: the Rofheart reference can repeat the inventive steps over a plurality of device (para 102), The Lundkvist reference processes teach an encryption/decryption of messages & subsequently validated (see Figures) and the Willey reference does teach mutual key agreement and mutual digit agreement before securely transmitting the link key.

Despite the non-entry of the after-final response, it is urged the undersigned contact the Examiner to advance prosecution.

36

INTERNATIONAL STANDARD

ISO/IEC 9798-1

Second edition
1997-08-01

Information technology — Security techniques — Entity authentication —

Part 1:
General

Technologies de l'information — Techniques de sécurité — Authentification d'entité —

Partie 1: Généralités

Reference number
ISO/IEC 9798-1:1997(E)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

International Standard ISO/IEC 9798-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC27, *IT Security techniques.*

This second edition cancels and replaces the first edition (ISO/IEC 9798-1:1991), which has been technically revised.

ISO/IEC 9798 consists of the following part, under the general title *Information technology — Security techniques — Entity authentication mechanisms*:

- *Part 3: Entity authentication using a public key algorithm*

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication*:

- *Part 1: General*
- *Part 2: Mechanisms using symmetric encipherment algorithms*
- *Part 4: Mechanisms using a cryptographic check function*
- *Part 5: Mechanisms using asymmetric zero knowledge techniques*

> NOTE — The introductory element of the title of part 3 will be aligned with the introductory element of the titles of parts 1, 2, 4 and 5 at the next revision of part 3 of ISO/IEC 9798.

Further parts may follow.

Annexes A, B, C and D of this part of ISO/IEC 9798 are for information only.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

Information technology — Security techniques — Entity authentication — Part 1: General

1 Scope

This part of ISO/IEC 9798 specifies an authentication model and general requirements and constraints for entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities, and where required, exchanges with a trusted third party.

The details of the mechanisms and the contents of the authentication exchanges are not specified in this part of ISO/IEC 9798 but in the subsequent parts.

Certain of the mechanisms specified in subsequent parts of ISO/IEC 9798 can be used to help provide non-repudiation services, mechanisms for which are specified in ISO/IEC 13888. The provision of non-repudiation services is beyond the scope of ISO/IEC 9798.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2: 1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model – Part 2: Security Architecture.*

ISO/IEC 9594-8: 1995, *Information technology — Open Systems Interconnection — The Directory — Part 8: Authentication framework.*

ISO/IEC 10181-2: 1996, *Information technology — Open Systems Interconnection Security frameworks for open systems: Authentication framework.*

ISO/IEC 13888-1 —[1]: *Information technology — Security techniques — Non-repudiation— Part 1: General.*

3 Definitions

3.1 ISO/IEC 9798 makes use of the following general security-related terms defined in ISO 7498-2:

3.1.1 cryptographic check value: information which is derived by performing a cryptographic transformation on the data unit.

3.1.2 masquerade: the pretence by an entity to be a different entity.

3.1.3 digital signature (signature): data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

3.2 ISO/IEC 9798 makes use of the following general security-related terms defined in ISO/IEC 10181-2:

3.2.1 claimant: an entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

3.2.2 principal: an entity whose identity can be authenticated.

[1] to be published

3.2.3 trusted third party: a security authority or its agent, trusted by other entities with respect to security-related activities. In the context of ISO/IEC 9798, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication.

3.2.4 verifier: an entity which is or represents the entity requiring an authenticated identity. A verifier includes the functions necessary for engaging in authentication exchanges.

3.3 For the purposes of ISO/IEC 9798 the following definitions apply:

3.3.1 asymmetric cryptographic technique: a cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

NOTE — A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques there are four elementary transformations: sign and verify for signature systems, encipher and decipher for encipherment systems. The signature and decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformation are published. There exist asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, since this is not the general case, throughout ISO/IEC 9798 the four elementary transformations and the corresponding keys are kept separate.

3.3.2 asymmetric encipherment system: a system based on asymmetric cryptographic techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment.

3.3.3 asymmetric key pair: a pair of related keys where the private key defines the private transformation and the public key defines the public transformation.

3.3.4 asymmetric signature system: a system based on asymmetric cryptographic techniques whose private transformation is used for signing and whose public transformation is used for verification.

3.3.5 challenge: a data item chosen at random and sent by the verifier to the claimant, which is used by the claimant, in conjunction with secret information held by the claimant, to generate a response which is sent to the verifier.

3.3.6 ciphertext: data which has been transformed to hide its information content.

3.3.7 cryptographic check function: a cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall be infeasible.

3.3.8 decipherment: the reversal of a corresponding encipherment.

3.3.9 distinguishing identifier: information which unambiguously distinguishes an entity.

3.3.10 encipherment: the (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data.

3.3.11 entity authentication: the corroboration that an entity is the one claimed.

3.3.12 interleaving attack: a masquerade which involves use of information derived from one or more ongoing or previous authentication exchanges.

3.3.13 key: a sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

3.3.14 mutual authentication: entity authentication which provides both entities with assurance of each other's identity.

3.3.15 plaintext: unenciphered information.

3.3.16 private decipherment key: private key which defines the private decipherment transformation.

3.3.17 private key: that key of an entity's asymmetric key pair which should only be used by that entity.

NOTE — In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation.

3.3.18 private signature key: private key which defines the private signature transformation.

NOTE — This is sometimes referred to as a secret signature key.

3.3.19 public encipherment key: public key which defines the public encipherment transformation.

3.3.20 public key: that key of an entity's asymmetric key pair which can be made public.

NOTE — In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a prespecified group.

3.3.21 public key certificate (certificate): the public key information of an entity signed by the certification authority and thereby rendered unforgeable (see also Annex C).

3.3.22 public key information: information specific to a single entity and which contains at least the entity's distinguishing identifier and at least one public key for this entity. There may be other information regarding the certification authority, the entity, and the public key included in the public key information, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms (see also Annex C).

3.3.23 public verification key: public key which defines the public verification transformation.

3.3.24 random number: a time variant parameter whose value is unpredictable (see also Annex B).

3.3.25 reflection attack: a masquerade which involves sending a previously transmitted message back to its originator.

3.3.26 replay attack: a masquerade which involves use of previously transmitted messages.

3.3.27 sequence number: a time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period (see also Annex B).

3.3.28 symmetric cryptographic technique: a cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

3.3.29 symmetric encipherment algorithm: an encipherment algorithm that uses the same secret key for both the originator's and the recipient's transformation.

3.3.30 time stamp: a time variant parameter which denotes a point in time with respect to a common reference (see also Annex B).

3.3.31 time variant parameter: a data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp (see also Annex B).

3.3.32 token: a message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique.

3.3.33 unilateral authentication: entity authentication which provides one entity with assurance of the other's identity but not vice versa.

4 Notation

Throughout ISO/IEC 9798 the following notation is used:

A: the distinguishing identifier of entity A.

B: the distinguishing identifier of entity B.

TP: the distinguishing identifier of the trusted third party.

K_{XY}: a secret key shared between entities X and Y, used only in symmetric cryptographic techniques.

P_X: a public verification key associated with entity X, used only in asymmetric cryptographic techniques.

S_X: a private signature key associated with entity X, used only in asymmetric cryptographic techniques.

N_X: a sequence number issued by entity X.

R_X: a random number issued by entity X.

T_X: a time stamp issued by entity X.

$^{T_X}_{N_X}$: a time variant parameter originated by entity X which is either a time stamp T_X or a sequence number N_X .

$Y||Z$: the result of the concatenation of the data items Y and Z in that order.

$eK(Z)$: the result of the encipherment of data Z with a symmetric encipherment algorithm using the key K.

$dK(Z)$: the result of the decipherment of data Z with a symmetric encipherment algorithm using the key K.

$f_K(Z)$: a cryptographic check value which is the result of applying the cryptographic check function f using as input a secret key K and an arbitrary data string Z.

CertX: a trusted third party's certificate for entity X.

TokenXY: a token sent from entity X to entity Y.

TVP: a time variant parameter.

$sS_X(Z)$: the signature resulting from applying the private signature transformation on data Z using the private signature key S_X.

5 Authentication model

The general model for entity authentication mechanisms is shown in Figure 1. It is not essential that all the entities and exchanges are present in every authentication mechanism.

For the authentication mechanisms specified in the other parts of ISO/IEC 9798, for unilateral authentication, entity A is considered the claimant, and entity B is considered the verifier. For mutual authentication, A and B each take the roles of both claimant and verifier.

For authentication purposes, the entities generate and exchange standardised messages, called tokens. It takes the exchange of at least one token for unilateral authentication and the exchange of at least two tokens for mutual authentication. An additional pass may be needed if a challenge has to be sent to initiate the authentication exchange. Additional passes may be needed if a trusted third party is involved.

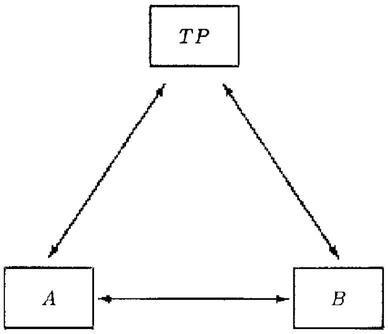


Figure 1 – Authentication model

In Figure 1, the lines indicate potential information flow. Entities A and B may either directly interact with each other, directly interact with the trusted third party TP, indirectly interact with the trusted third party through B or A respectively, or use some information issued by the trusted third party.

The details of the authentication mechanisms of ISO/IEC 9798 are specified in the subsequent parts.

6 General requirements and constraints

In order that an entity can authenticate another entity, both shall use a common set of cryptographic techniques and parameters.

During the operational life of a key, the values of all time-variant parameters on which the key operates (i.e., time stamps, sequence numbers, and random numbers) shall be non-repeating, at least with overwhelming probability.

It is assumed that, during use of an authentication mechanism, the entities A and B are aware of each other's claimed identities. This may be achieved by the inclusion of identifiers in information exchanged between the two entities, or it may be apparent from the context of the use of the mechanism.

The authenticity of the entity can be ascertained only for the instant of the authentication exchange. To guarantee the authenticity of subsequent communicated data, the authentication exchange must be used in conjunction with a secure means of communication (e.g., an integrity service).

Annex A

(informative)

Use of text fields

The tokens specified in the following parts of ISO/IEC 9798 contain text fields. The actual use of and the relationships between the various text fields in a given pass depend on the application.

Text fields may contain additional time variant parameters. For instance, a time stamp may be included in the text field(s) of a token if this is used with sequence numbers. This would allow the detection of forced delays by requiring the recipient of a message to verify that any time stamp contained in the message is within a prespecified time window (see also Annex B).

If more than one valid key exists, then an identifier of the key may be included in a text field in the plaintext. If more than one trusted third party exists, then text fields could be used to include the distinguishing identifier of the trusted third party in question.

Text fields could also be used for the distribution of keys (see ISO/IEC 11770-2 and ISO/IEC 11770-3).

Should any of the mechanisms specified in the following parts of ISO/IEC 9798 be embedded in an application which allows either entity to initiate the authentication by using an additional message prior to the start of the mechanism, certain intruder attacks may become possible. Text fields may be used to state which entity requests the authentication in order to counteract such attacks, which are characterized by the fact that an intruder may reuse a token obtained illicitly (see ISO/IEC 10181-2).

The above examples are not exhaustive.

Annex B
(informative)

Time variant parameters

Time variant parameters are used to control uniqueness/timeliness. They enable replay of previously transmitted messages to be detected. To achieve this, the authentication information should vary from one exchange instance to the next.

Some types of time variant parameters may also allow for the detection of "forced delays" (delays introduced into the communication medium by an adversary). In mechanisms involving more than one pass, forced delays may also be detected by other means (such as "timeout clocks" used to enforce maximum allowable time gaps between specific messages).

The three types of time variant parameters used in the following parts of ISO/IEC 9798 are time stamps, sequence numbers, and random numbers. Implementation requirements may make different time variant parameters preferable in different applications. In some cases, it may be appropriate to use more than one type of time variant parameter (e.g., both time stamps and sequence numbers). Details regarding the choice of these parameters are beyond the scope of this part of ISO/IEC 9798.

B.1 Time stamps

Mechanisms involving time stamps make use of a common time reference which logically links a claimant and a verifier. The recommended reference clock is Coordinated Universal Time (UTC). An acceptance window of some fixed size is used by the verifier. Timeliness is controlled by the verifier computing the difference between the time stamp in a verified received token and the time as perceived by the verifier at the time the token is received. If the difference is within the window, the message is accepted. Uniqueness can be verified by logging all messages within the current window, and rejecting the second and subsequent occurrences of identical messages within that window.

Some mechanism should be used to ensure that the time clocks of the communicating entities are synchronised. Moreover, time clocks need to be synchronized well enough to make the possibility of impersonation by replay acceptably small. It should also be ensured that all information relevant to the verification of time stamps, in particular the time clocks of the two communicating entities, are protected against tampering.

Mechanisms using time stamps allow the detection of forced delays.

B.2 Sequence numbers

Uniqueness can be controlled using sequence numbers as they enable a verifier to detect the replay of messages. A claimant and verifier agree beforehand on a policy for numbering messages in a particular manner, the general idea being that a message with a particular number will be accepted only once (or only once within a specified time period). Messages received by a verifier are then checked to see that the number sent along with the message is acceptable according to the agreed policy. A message is rejected if the accompanying sequence number is not in accordance with the agreed policy.

Use of sequence numbers may require additional "bookkeeping". A claimant should maintain records of sequence numbers which have been used previously and/or sequence numbers that remain valid for future use. The claimant should keep such records for all potential verifiers with whom the claimant may wish to communicate. Similarly, the verifier should maintain such records corresponding to all potential claimants. Special procedures may also be required to reset and/or restart sequence number counters when situations (such as system failures) arise which disrupt normal sequencing.

Use of sequence numbers by a claimant does not guarantee that a verifier will be able to detect forced delays. For mechanisms involving two or more messages, forced delays can be detected if the sender of a message measures the time interval between transmission of a message and receipt of an expected reply, and rejects it if the delay is more than a prespecified time slot.

B.3 Random numbers

The random numbers as used in mechanisms specified in the following parts of ISO/IEC 9798 prevent replay or interleaving attacks. It is therefore required that all random numbers used in ISO/IEC 9798 are chosen from a sufficiently large range so that the probability of repetition is very small when used with the same key, and also that the probability of a third party predicting a specific value is very small. In the context of ISO/IEC 9798, the use of the term random numbers also includes pseudorandom numbers satisfying the same requirements.

In order to prevent replay or interleaving attacks, the verifier obtains a random number which is sent to the claimant, and the claimant responds by including the random number in the protected part of the returned token. (This is commonly referred to as challenge-response.) This procedure links the two messages containing the particular random number. If the same random number were to be used by the verifier again, a third party that recorded the original authentication exchange could send the recorded token to the verifier and falsely authenticate itself as the claimant. The requirement that the random number be non-repeating with very high probability is present in order to prevent such attacks.

Use of random numbers by a claimant does not guarantee that a verifier will be able to detect forced delays.

Annex C
(informative)

Certificates

In the following parts of ISO/IEC 9798 public key certificates (certificates) can be used to ensure the authenticity of public keys. In this case, a certificate contains an entity's public key information, which consists of at least the entity's distinguishing identifier and public key. There may be other information included in the public key information regarding the certification authority, the entity, and the public key, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms. The certificate consists of the public key information signed by the trusted third party.

The verification of a certificate consists of verifying the signature of the trusted third party, and checking, if required, other conditions related to the validity of the certificate such as the revocation or the validity period.

Certificates are not the only way of guaranteeing the authenticity of public keys. To allow an entity to obtain the public keys of other entities by other means, the use of certificates is optional in all mechanisms in the following parts of ISO/IEC 9798. Other methods of guaranteeing the authenticity of public keys include identity-based signature schemes such as specified in ISO/IEC 14888-2.

Annex D

(informative)

Bibliography

[1] ISO/IEC 7498-1: 1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model.*

[2] ISO/IEC 9796: 1991, *Information technology — Security techniques — Digital signature scheme giving message recovery.*

[3] ISO/IEC 10181-1: 1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview.*

[4] ISO/IEC 11770-1: 1996, *Information technology — Security techniques — Key management — Part 1: Framework.*

[5] ISO/IEC 11770-2: 1996, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques.*

[6] ISO/IEC 11770-3 —[1]: *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques.*

[7] ISO/IEC 14888-1 —[1]: *Information technology — Security techniques — Digital signatures with appendix — Part 1: General.*

[8] ISO/IEC 14888-2 —[1]: *Information technology — Security techniques — Digital signatures with appendix — Part 2: Identity-based mechanisms.*

[9] ISO/IEC 14888-3 —[1]: *Information technology — Security techniques — Digital signatures with appendix — Part 3: Certificate-based mechanisms.*

[1] to be published

ICS 35.040

Descriptors: data processing, information interchange, protection of information, security techniques, authentication, message authentication codes, models.

Price based on 9 pages

INTERNATIONAL STANDARD

ISO/IEC 9798-2

Second edition
1999-07-15

Information technology — Security techniques — Entity authentication —

Part 2:
Mechanisms using symmetric encipherment algorithms

Technologies de l'information — Techniques de sécurité — Authentification d'entité —

Partie 2: Mécanismes utilisant des algorithmes de chiffrement symétriques

ISO IEC

Reference number
ISO/IEC 9798-2:1999(E)

Contents

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 9798-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 9798-2:1994), which has been technically revised. Note, however, that implementations which comply with ISO/IEC 9798-2 (1st edition) will be compliant with ISO/IEC 9798-2 (2nd edition).

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication*:

— *Part 1: General*

— *Part 2: Mechanisms using symmetric encipherment algorithms*

— *Part 3: Mechanisms using digital signature techniques*

— *Part 4: Mechanisms using a cryptographic check function*

— *Part 5 : Mechanisms using zero knowledge techniques*

Further parts may follow.

Annex A of this part of ISO/IEC 9798 is for information only.

Information technology — Security techniques — Entity authentication —

Part 2:
Mechanisms using symmetric encipherment algorithms

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using symmetric encipherment algorithms. Four of the mechanisms provide entity authentication between two entities where no trusted third party is involved; two of these are mechanisms to unilaterally authenticate one entity to another, while the other two are mechanisms for mutual authentication of two entities. The remaining mechanisms require a trusted third party for the establishment of a common secret key, and realize mutual or unilateral entity authentication.

The mechanisms specified in this part of ISO/IEC 9798 use time variant parameters such as time stamps, sequence numbers, or random numbers, to prevent valid authentication information from being accepted at a later time or more than once.

If no trusted third party is involved and a time stamp or sequence number is used, one pass is needed for unilateral authentication, while two passes are needed to achieve mutual authentication. If no trusted third party is involved and a challenge and response method employing random numbers is used, two passes are needed for unilateral authentication, while three passes are required to achieve mutual authentication. If a trusted third party is involved, any additional communication between an entity and the trusted third party requires two extra passes in the communication exchange.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9798-1:1997, *Information technology — Security techniques — Entity authentication — Part 1: General.*

ISO/IEC 11770-2:1996, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques.*

3 Definitions and notation

For the purposes of this part of ISO/IEC 9798, the definitions and notation described in ISO/IEC 9798-1 apply.

4 Requirements

In the authentication mechanisms specified in this part of ISO/IEC 9798 an entity to be authenticated corroborates its identity by demonstrating its knowledge of a secret authentication key. This is achieved by the entity using its secret key to encipher specific data. The enciphered data can be deciphered by anyone sharing the entity's secret authentication key.

The authentication mechanisms have the following requirements. If any one of these is not met then the authentication process may be compromised or it cannot be implemented.

a) A claimant authenticating itself to a verifier shall share a common secret authentication key with that verifier, in which case the mechanisms of clause 5 apply, or each entity shall share a secret authentication key with a common trusted third party, in which case the mechanisms of clause 6 apply. Such keys shall be known to the involved parties prior to the commencement of any particular run of an authentication mechanism. The method by which this is achieved is beyond the scope of this part of ISO/IEC 9798.

b) If a trusted third party is involved it shall be trusted by both the claimant and the verifier.

c) The secret authentication key shared by a claimant and a verifier, or by an entity and a trusted third party, shall be known only to those two parties and, possibly, to other entities they both trust.

NOTE 1 The encipherment algorithm and the key lifetime should be chosen so that it is computationally infeasible for a key to be deduced during its lifetime. In addition, the key lifetime should be chosen to prevent known plaintext or chosen plaintext attacks.

a) For every possibility for the secret key *K*, the encipherment function *eK* and its corresponding decipherment function *dK* shall have the following property. The decipherment process *dK*, when applied to a string *eK*(*X*), shall enable the recipient of that string to detect forged or manipulated data, i.e. only the possessor of the secret key *K* shall be capable of generating strings which will be 'accepted' when subjected to the decipherment process *dK*.

NOTE 2 In practice, this can be achieved in many ways. Two examples are as follows.

1. If sufficient redundancy is present in, or appended to, the data, and the encipherment algorithm is chosen with care, the integrity requirement can be satisfied. The redundancy is checked for correctness by the recipient before the deciphered data can be accepted as valid.

2. The key *K* is used to derive a pair of keys *K'* and *K''*. The key *K''* is then used to calculate a Message Authentication Code (MAC) on the data to be enciphered, while the key *K'* is used to encipher the data concatenated with the MAC. The recipient checks that the value of the MAC is correct before accepting the deciphered data as valid.

a) The mechanisms in this part of ISO/IEC 9798 require the use of time variant parameters such as time stamps, sequence numbers or random numbers. The properties of these parameters, in particular that it is most unlikely for them to repeat within the lifetime of a secret authentication key, are important for the security of these mechanisms. For additional information see annex B of ISO/IEC 9798-1.

5 Mechanisms not involving a trusted third party

In these authentication mechanisms the entities *A* and *B* shall share a common secret authentication key K_{AB} or two unidirectional secret keys K_{AB} and K_{BA} prior to the commencement of any particular run of the authentication mechanisms. In the latter case the unidirectional keys K_{AB} and K_{BA} are used respectively for the authentication of *A* by *B* and of *B* by *A*.

All text fields specified in the following mechanisms are available for use in applications outside the scope of this part of ISO/IEC 9798 (they may be empty). Their relationship and contents depend upon the specific application. See annex A for information on the use of text fields.

5.1 Unilateral authentication

Unilateral authentication means that only one of the two entities is authenticated by use of the mechanism.

5.1.1 One pass authentication

In this authentication mechanism the claimant *A* initiates the process and is authenticated by the verifier *B*. Uniqueness/timeliness is controlled by generating and checking a time stamp or a sequence number (see annex B of ISO/IEC 9798-1). The authentication mechanism is illustrated in Figure 1.

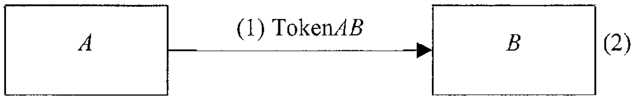


Figure 1

The form of the token (Token*AB*), sent by the claimant *A* to the verifier *B* is:

$$\text{Token}AB = \text{Text2} \,||\, eK_{AB}(\begin{matrix}T_A\\ N_A\end{matrix} \,||\, B \,||\, \text{Text1})$$

where the claimant *A* uses either a sequence number N_A or a time stamp T_A as the time variant parameter. The choice depends on the technical capabilities of the claimant and the verifier as well as on the environment.

The inclusion of the distinguishing identifier *B* in Token*AB* is optional.

NOTE Distinguishing identifier *B* is included in Token*AB* to prevent the re-use of Token*AB* on entity *A* by an adversary masquerading as entity *B*. Its inclusion is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier *B* may also be omitted if a unidirectional key is used.

(1) *A* generates and sends Token*AB* to *B*.

(2) On receipt of the message containing Token*AB*, *B* verifies Token*AB* by deciphering the enciphered part (where deciphering implies that the requirements of 4.d are met) and then checking the correctness of the distinguishing identifier *B*, if present, as well as the time stamp or the sequence number.

5.1.2 Two pass authentication

In this authentication mechanism the claimant *A* is authenticated by the verifier *B* who initiates the process. Uniqueness/timeliness is controlled by generating and checking a random number R_B (see annex B of ISO/IEC 9798-1). The authentication mechanism is illustrated in Figure 2.

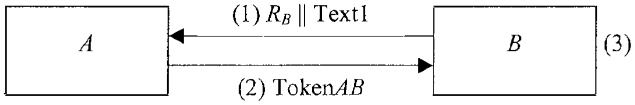


Figure 2

The form of the token (Token*AB*), sent by the claimant *A* to the verifier *B* is:

$$\text{Token}AB = \text{Text3} \,||\, eK_{AB}(R_B \,||\, B \,||\, \text{Text2}).$$

The inclusion of the distinguishing identifier *B* in Token*AB* is optional.

NOTE 1 In order to prevent the possibility of a known plaintext attack, i.e. a cryptanalytic attack where the cryptanalyst knows the complete plaintext for one or more ciphertext strings, entity *A* may include a random number R_A in Text2.

NOTE 2 Distinguishing identifier *B* is included in Token*AB* to prevent a so-called reflection attack. Such an attack is characterised by the fact that an intruder 'reflects' the challenge R_B to *B* pretending to be *A*. The inclusion of the distinguishing identifier *B* is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier *B* may also be omitted if a unidirectional key is used.

(1) *B* generates a random number R_B and sends it and, optionally, a text field Text1 to *A*.

(2) *A* generates and sends Token*AB* to *B*.

(3) On receipt of the message containing Token*AB*, *B* verifies Token*AB* by deciphering the enciphered part (where deciphering implies that the requirements of 4.d are met) and then checking the correctness of the distinguishing identifier *B*, if present, and that the random number R_B, sent to *A* in step (1), agrees with the random number contained in Token*AB*.

5.2 Mutual authentication

Mutual authentication means that the two communicating entities are authenticated to each other by use of the mechanism.

The two mechanisms described in 5.1.1 and 5.1.2 are adapted in 5.2.1 and 5.2.2, respectively, to achieve mutual authentication. In both cases this requires one more pass and results in two more steps.

NOTE A third mechanism for mutual authentication can be constructed from two instances of the mechanism specified in 5.1.2, one started by entity *A* and the other by entity *B*.

5.2.1 Two pass authentication

In this authentication mechanism uniqueness/timeliness is controlled by generating and checking time stamps or sequence numbers (see annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in Figure 3.

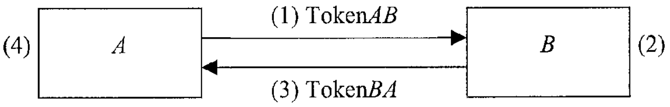


Figure 3

The form of the token (Token*AB*), sent by *A* to *B*, is identical to that specified in 5.1.1.

$$\text{Token}AB = \text{Text2} \,\|\, eK_{AB}(\begin{matrix}T_A\\N_A\end{matrix} \,\|\, B \,\|\, \text{Text1}).$$

The form of the token (Token*BA*), sent by *B* to *A*, is:

$$\text{Token}BA = \text{Text4} \,\|\, eK_{AB}(\begin{matrix}T_B\\N_B\end{matrix} \,\|\, A \,\|\, \text{Text3}).$$

The inclusion of the distinguishing identifier *B* in Token*AB* and the inclusion of the distinguishing identifier *A* in Token*BA* are (independently) optional.

NOTE 1 Distinguishing identifier *B* is included in Token*AB* to prevent the re-use of Token*AB* on entity *A* by an adversary masquerading as entity *B*. For similar reasons the distinguishing identifier *A* is present in Token*BA*. Their inclusion is made optional so that, in environments where such attacks cannot occur, one or both may be omitted.

The distinguishing identifiers *A* and *B* may also be omitted if unidirectional keys (see below) are used.

The choice of using either time stamps or sequence numbers in this mechanism depends on the capabilities of the claimant and the verifier as well as on the environment.

Steps (1) and (2) are identical to those specified in 5.1.1, one pass authentication.

(3) *B* generates and sends Token*BA* to *A*.

(4) The message in step (3) is handled in a manner analogous to step (2) of 5.1.1.

NOTE 2 The two messages of this mechanism are not bound together in any way, other than implicitly by timeliness; the mechanism involves independent use of mechanism 5.1.1 twice. Further binding together of these messages can be achieved by making appropriate use of text fields.

If unidirectional keys are used then the key K_{AB} in Token*BA* is replaced by the unidirectional key K_{BA}, and the appropriate key is used in step (4).

5.2.2 Three pass authentication

In this authentication mechanism uniqueness/timeliness is controlled by generating and checking random numbers (see annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in Figure 4.

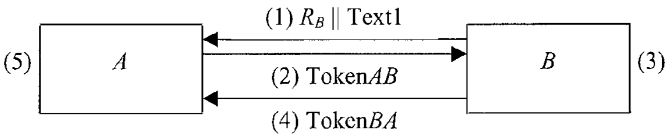


Figure 4

The tokens are of the following form:

$$\text{Token}AB = \text{Text3} \,||\, eK_{AB}(R_A \,||\, R_B \,||\, B \,||\, \text{Text2}),$$

$$\text{Token}BA = \text{Text5} \,||\, eK_{AB}(R_B \,||\, R_A \,||\, \text{Text4}).$$

The inclusion of the distinguishing identifier *B* in Token*AB* is optional.

NOTE When present, distinguishing identifier *B* is included in Token*AB* to prevent a so-called reflection attack. Such an attack is characterized by the fact that an intruder 'reflects' the challenge R_B to *B* pretending to be *A*. The inclusion of the distinguishing identifier *B* is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier *B* may also be omitted if unidirectional keys (see below) are used.

(1) *B* generates a random number R_B and sends it and, optionally, a text field Text1 to *A*.

(2) *A* generates a random number R_A, and generates and sends Token*AB* to *B*.

(3) On receipt of the message containing Token*AB*, *B* verifies Token*AB* by deciphering the enciphered part (where deciphering implies that the requirements of 4.d are met) and then checking the correctness of the distinguishing identifier *B*, if present, and that the random number R_B, sent to *A* in step (1), agrees with the random number contained in Token*AB*.

(4) *B* generates and sends Token*BA* to *A*.

(5) On receipt of the message containing Token*BA*, *A* verifies Token*BA* by deciphering the enciphered part (where deciphering implies that the requirements of 4.d are met) and then checking that the random number R_B, received from *B* in step (1) agrees with the random number contained in Token*BA* and that the random number R_A, sent to *B* in step (2), agrees with the random number contained in Token*BA*.

If unidirectional keys are used then the key K_{AB} in Token*BA* is replaced by the unidirectional key K_{BA}, and the appropriate key is used in step (5).

6 Mechanisms involving a trusted third party

The authentication mechanisms in this clause do not make use of a secret key shared by the two entities prior to the authentication process. They do, however, make use of a trusted third party (with distinguishing identifier *TP*) with which the entities *A* and *B* each share a secret key, K_{AT} and K_{BT} respectively. In each mechanism one of the entities requests a key K_{AB} from the trusted third party. This is followed by an adaptation of the mechanisms described in 5.2.1 and 5.2.2, respectively.

As described below certain passes may be omitted from each mechanism if only unilateral authentication is required.

All text fields specified in the following mechanisms are available for use in applications outside the scope of this part of ISO/IEC 9798 (they may be empty). Their relationship and contents depend upon the specific application. See annex A for information on the use of text fields.

6.1 Four pass authentication

In this mutual authentication mechanism uniqueness/timeliness is controlled by using time variant parameters (see annex B of ISO/IEC 9798-1). This mechanism is equivalent to Key Establishment Mechanism 8 of ISO/IEC 11770-2: 1996.

The authentication mechanism is illustrated in Figure 5.

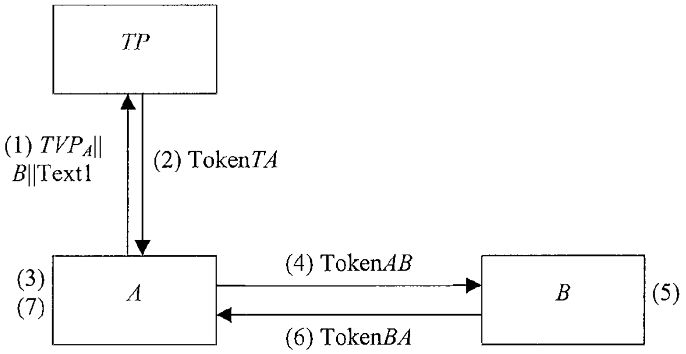


Figure 5

The form of the token (Token*TA*), sent by *TP* to *A*, is:

$$\text{Token}TA = \text{Text4} \,||\, eK_{AT}(TVP_A \,||\, K_{AB} \,||\, B \,||\, \text{Text3}) \,||\, eK_{BT}(\begin{matrix}T_{TP}\\N_{TP}\end{matrix} \,||\, K_{AB} \,||\, A \,||\, \text{Text2})\,.$$

The form of the token (Token*AB*), sent by *A* to *B*, is:

$$\text{Token}AB = \text{Text6} \,\|\, eK_{BT}(\genfrac{}{}{0pt}{}{T_{TP}}{N_{TP}} \,\|\, K_{AB} \,\|\, A \,\|\, \text{Text2}) \,\|\, eK_{AB}(\genfrac{}{}{0pt}{}{T_{A}}{N_{A}} \,\|\, B \,\|\, \text{Text5}) .$$

The form of the token (Token*BA*), sent by *B* to *A*, is:

$$\text{Token}BA = \text{Text8} \,\|\, eK_{AB}(\genfrac{}{}{0pt}{}{T_{B}}{N_{B}} \,\|\, A \,\|\, \text{Text7}) .$$

The choice of using either time stamps or sequence numbers in this mechanism depends on the capabilities of the entities involved as well as on the environment.

The use of the time variant parameter TVP_A in steps (1) through (3) of figure 5, as specified below, is somewhat different from its normal use. It allows *A* to associate the response message (2) with the message request (1). The important property of the time variant parameter here is its non-repeatability, to limit the possible re-use of a previously used Token*TA*.

NOTE The time variant parameter TVP_A could be a random number. However, unlike the random numbers used in certain of the mechanisms in this part of ISO/IEC 9798, it is not necessary that TVP_A be unpredictable to a third party, and a non-repeating counter value would be equally appropriate.

(1) *A* generates a time variant parameter TVP_A, and sends it, the distinguishing identifier *B* and, optionally, a text field Text1 to the trusted third party *TP*.

(2) The trusted third party *TP* generates and sends Token*TA* to *A*.

(3) On receipt of the message containing Token*TA*, *A* verifies Token*TA* by deciphering the data enciphered under K_{AT} (where deciphering implies that the requirements of 4.d are met) and then checking the correctness of the distinguishing identifier *B* and that the time variant parameter, sent to *TP* in step (1), agrees with the time variant parameter contained in Token*TA*. In addition, *A* retrieves the secret authentication key K_{AB}. *A* then extracts

$$eK_{BT}(\genfrac{}{}{0pt}{}{T_{TP}}{N_{TP}} \,\|\, K_{AB} \,\|\, A \,\|\, \text{Text2})$$

from Token*TA* and uses it to construct Token*AB*.

(4) *A* generates and sends Token*AB* to *B*.

(5) On receipt of the message containing Token*AB*, *B* verifies Token*AB* by deciphering the enciphered parts (where deciphering implies that the requirements of 4.d are met) and then checking the correctness of the distinguishing identifiers *A* and *B* as well as the time stamp(s) or the sequence number(s). In addition, *B* retrieves the secret authentication key K_{AB}.

(6) *B* generates and sends Token*BA* to *A*.

(7) On receipt of the message containing Token*BA*, *A* verifies Token*BA* by deciphering the enciphered part (where deciphering implies that the requirements of 4.d are met) and then checking the correctness of the distinguishing identifier *A* as well as the time stamp or the sequence number.

Steps (6) and (7) may be omitted if only unilateral authentication of *A* to *B* is required.

6.2 Five pass authentication

In this mutual authentication mechanism uniqueness/timeliness is controlled by using random numbers (see annex B of ISO/IEC 9798-1). This mechanism is equivalent to Key Establishment Mechanism 9 of ISO/IEC 11770-2: 1996.

The authentication mechanism is illustrated in Figure 6.

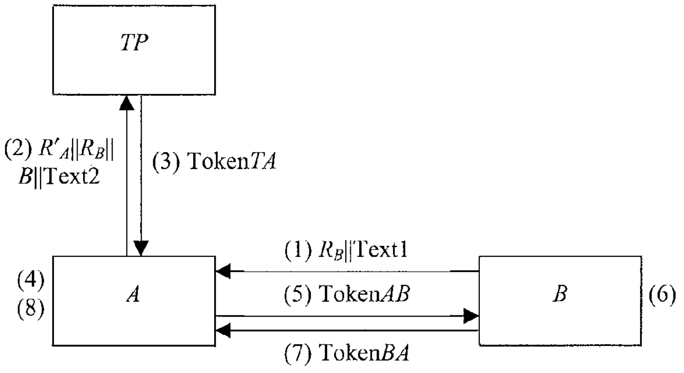


Figure 6

The form of the token (Token*TA*), sent by *TP* to *A*, is:

$$\text{Token}TA = \text{Text5} \,\|\, eK_{AT}(R'_A \,\|\, K_{AB} \,\|\, B \,\|\, \text{Text4}) \,\|\, eK_{BT}(R_B \,\|\, K_{AB} \,\|\, A \,\|\, \text{Text3}) .$$

The form of the token (Token*AB*), sent by *A* to *B*, is:

$$\text{Token}AB = \text{Text7} \,\|\, eK_{BT}(R_B \,\|\, K_{AB} \,\|\, A \,\|\, \text{Text3}) \,\|\, eK_{AB}(R_A \,\|\, R_B \,\|\, \text{Text6}) .$$

The form of the token (Token*BA*), sent by *B* to *A*, is:

$$\text{Token}BA = \text{Text9} \,\|\, eK_{AB}(R_B \,\|\, R_A \,\|\, \text{Text8}) .$$

(1) *B* generates a random number R_B and sends it and, optionally, a text field Text1 to *A*.

(2) *A* generates a random number R'_A and sends it, the random number R_B, the distinguishing identifier *B* and, optionally, a text field Text2 to the trusted third party *TP*.

(3) The trusted third party *TP* generates and sends Token*TA* to *A*.

(4) On receipt of the message containing Token*TA*, *A* verifies Token*TA* by deciphering the data enciphered under K_{AT} (where deciphering implies that the requirements of 4.d are met) and then checking the correctness of the distinguishing identifier *B* and that the random number R'_A, sent to *TP* in step (2), agrees with the random number contained in Token*TA*. In addition, *A* retrieves the secret authentication key K_{AB}. *A* then extracts

$$eK_{BT}(R_B \,\|\, K_{AB} \,\|\, A \,\|\, \text{Text3})$$

from Token*TA* and uses it to construct Token*AB*.

(5) *A* generates a second random number R_A, and generates and sends Token*AB* to *B*.

(6) On receipt of the message containing Token*AB*, *B* verifies Token*AB* by deciphering the enciphered parts (where deciphering implies that the requirements of 4.d are met) and then checking the correctness of the distinguishing identifier *A* and that the random number R_B, sent to *A* in step (1), agrees with both copies contained in Token*AB*. In addition, *B* retrieves the secret authentication key K_{AB}.

(7) *B* generates and sends Token*BA* to *A*.

(8) On receipt of the message containing Token*BA*, *A* verifies Token*BA* by deciphering the enciphered part (where deciphering implies that the requirements of 4.d are met) and then checking that the random number R_B, received from *B* in step (1), agrees with the random number contained in Token*BA* and that the random number R_A, sent to *B* in step (5), agrees with the random number contained in Token*BA*.

Steps (7) and (8) may be omitted if only unilateral authentication of *A* to *B* is required.

Annex A
(informative)

Use of text fields

The tokens specified in clauses 5 and 6 of this part of ISO/IEC 9798 contain text fields. The actual use of and the relationships between the various text fields in a given pass depend on the application. Some examples are given below; see also annex A of ISO/IEC 9798-1.

If the tokens do not contain (sufficient) redundancy, the enciphered text fields may be used to provide additional redundancy.

Any information requiring confidentiality or data origin authentication should be placed in the enciphered part of the token.

Bibliography

[1] ISO/IEC 9797: 1994, *Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.*

[2] ISO/IEC 10118-1: 1994, *Information technology — Security techniques — Hash-functions — Part 1: General.*

[3] ISO/IEC 10118-2: 1994, *Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher algorithm.*

ICS 35.040

Price based on 11 pages

INTERNATIONAL STANDARD

ISO/IEC 9798-3

Second edition
1998-10-15

Information technology — Security techniques — Entity authentication —

Part 3:
Mechanisms using digital signature techniques

Technologies de l'information — Techniques de sécurité — Authentification d'entité —

Partie 3: Mécanismes utilisant des techniques de signature numériques

Reference number
ISO/IEC 9798-3:1998(E)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee. ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

International Standard ISO/IEC 9798–3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC27, *IT Security techniques.*

This second edition cancels and replaces the first edition (ISO/IEC 9798-3:1993), which has been technically revised. Note, however, that implementations which comply with ISO/IEC 9798-3 (1st edition) will be compliant with ISO/IEC 9798-3 (2nd edition).

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication*:

- *Part 1: General*
- *Part 2: Mechanisms using symmetric encipherment algorithms*
- *Part 3: Mechanisms using digital signature techniques*
- *Part 4: Mechanisms using a cryptographic check function*
- *Part 5: Mechanisms using zero knowledge techniques*

Further parts may follow.

Annex A of this part of ISO/IEC 9798 is for information only.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

Information technology — Security techniques — Entity authentication —

Part 3:

Mechanisms using digital signature techniques

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using digital signatures based on asymmetric techniques. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities. A digital signature is used to verify the identity of an entity. A trusted third party may be involved.

The mechanisms specified in this part of ISO/IEC 9798 use time variant parameters such as time stamps, sequence numbers, or random numbers, to prevent valid authentication information from being accepted at a later time.

If a time stamp or a sequence number is used, one pass is needed for unilateral authentication, while two passes are needed to achieve mutual authentication. If a challenge and response method employing random numbers is used, two passes are needed for unilateral authentication, while three or four passes (depending on the mechanism employed) are required to achieve mutual authentication.

2 Normative reference

The following standard contains provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. At the time of publication, the edition indicated was valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 9798-1: 1997, *Information technology — Security techniques — Entity authentication — Part 1: General.*

3 Definitions and notation

For the purposes of this part of ISO/IEC 9798 the definitions and notation described in ISO/IEC 9798-1 apply.

4 Requirements

In the authentication mechanisms specified in this part of ISO/IEC 9798 an entity to be authenticated corroborates its identity by demonstrating its knowledge of its private signature key. This is achieved by the entity using its private signature key to sign specific data. The signature can be verified by anyone using the entity's public verification key.

The authentication mechanisms have the following requirements:

a) A verifier shall possess the valid public key of the claimant, i.e., of the entity that the claimant claims to be.

b) A claimant shall have a private signature key known and used only by the claimant.

If either of these is not satisfied then the authentication process may be compromised or it cannot be completed successfully.

NOTES

1 One way of obtaining a valid public key is by means of a certificate (see Annex C of ISO/IEC 9798-1). The generation, distribution, and revocation of certificates are outside the scope of this part of ISO/IEC 9798. There may exist a trusted third party for this purpose. Another way of obtaining a valid public key is by trusted courier.

2 References to digital signature schemes are contained in Annex D of ISO/IEC 9798-1.

5 Mechanisms

The specified entity authentication mechanisms make use of time variant parameters such as time stamps, sequence numbers or random numbers (see Annex B of ISO/IEC 9798-1 and Note 1 below).

Throughout this part of ISO/IEC 9798, tokens have the following form:

$$\text{Token} = X_1||\cdots||X_i||sS_A(Y_1||\cdots||Y_j).$$

In this part of ISO/IEC 9798, the term "signed data" refers to "$Y_1||\cdots||Y_j$" used as input to the signature scheme and the term "unsigned data" refers to "$X_1||\cdots||X_i$".

If information contained in the signed data of the token can be recovered from the signature, then it need not be contained in the unsigned data of the token (see, for example, ISO/IEC 9796).

If information contained in the text field of the signed data of the token cannot be recovered from the signature, then it shall be contained in the unsigned text field of the token.

If information in the signed data of the token (e.g., a random number) is already known to the verifier, then it need not be contained in the unsigned data of the token sent by the claimant.

All text fields specified in the following mechanisms are available for use in applications outside the scope of this part of ISO/IEC 9798 (they may be empty). Their relationship and contents depend upon the specific application. See Annex A for information on the use of text fields.

NOTES

1 The signing by one entity of a data block which has been manipulated by a second entity for some ulterior motive can be prevented by the first entity including its own random number in the data block which it signs. In this case, it is the unpredictability which prevents the signing of pre-defined data.

2 As the distribution of certificates is outside the scope of this part of ISO/IEC 9798, the sending of certificates is optional in all mechanisms.

5.1 Unilateral authentication

Unilateral authentication means that only one of the two entities is authenticated by use of the mechanism.

5.1.1 One pass authentication

In this authentication mechanism the claimant A initiates the process and is authenticated by the verifier B. Uniqueness / timeliness is controlled by generating and checking a time stamp or a sequence number (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 1.

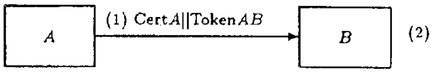


Figure 1

The form of the token (TokenAB), sent by the claimant A to the verifier B is:

$$\text{Token}AB = {}^{T_A}_{N_A}||B||\text{Text2}||sS_A\left({}^{T_A}_{N_A}||B||\text{Text1}\right),$$

where the claimant A uses either a sequence number N_A or a time stamp T_A as the time variant parameter. The choice depends on the technical capabilities of the claimant and the verifier as well as on the environment

NOTES

1 The inclusion of the identifier B in the signed data of TokenAB is necessary to prevent the token from being accepted by anyone other than the intended verifier.

2 In general, Text2 is not authenticated by this process.

3 One application of this mechanism could be key distribution (see Annex A of ISO/IEC 9798-1).

(1) A sends TokenAB and, optionally, its certificate to B.

(2) On receipt of the message containing TokenAB, B performs the following steps:

  (i) It ensures that it is in possession of a valid public key of A either by verifying the certificate of A or by some other means.

  (ii) It verifies TokenAB by verifying the signature of A contained in the token, by checking the time stamp or the sequence number, and by checking that the value of the identifier field (B) in the signed data of TokenAB is equal to entity B's distinguishing identifier.

5.1.2 Two pass authentication

In this authentication mechanism the claimant A is authenticated by the verifier B who initiates the process. Uniqueness / timeliness is controlled by generating and checking a random number R_B (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 2.

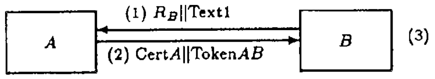


Figure 2

The form of the token (TokenAB), sent by the claimant A to the verifier B is:

$$\text{Token}AB = R_A||R_B||B||\text{Text3}||sS_A\,(R_A||R_B||B||\text{Text2}).$$

The inclusion of identifier B in TokenAB is optional. It depends on the environment in which this authentication mechanism is used.

NOTES

1 The inclusion of the optional identifier B in the signed data of TokenAB can prevent the token from being accepted by anyone other than the intended verifier (e.g., in a person-in-the-middle attack).

2 The inclusion of the random number R_A in the signed part of TokenAB prevents B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This measure may be required, for example, when the same key is used by A for purposes other than entity authentication.

(1) B sends a random number R_B and, optionally, a text field Text1 to A.

(2) A sends TokenAB and, optionally, its certificate to B.

(3) On receipt of the message containing TokenAB, B performs the following steps:

(i) It ensures that it is in possession of a valid public key of A either by verifying the certificate of A or by some other means.

(ii) It verifies TokenAB by checking the signature of A contained in the token, by checking that the random number R_B, sent to A in step (1), agrees with the random number contained in the signed data of TokenAB, and by checking that the value of the identifier field (B) in the signed data of TokenAB, if present, is equal to B's distinguishing identifier.

5.2 Mutual authentication

Mutual authentication means that the two communicating entities are authenticated to each other.

The two mechanisms described in 5.1.1 and 5.1.2 are extended in 5.2.1 and 5.2.2, respectively, to achieve mutual authentication. This is done by transmitting one further message resulting in two additional steps.

The mechanism specified in 5.2.3 uses four messages which, however, need not all be sent consecutively. In this way the authentication process may be speeded up.

5.2.1 Two pass authentication

In this authentication mechanism uniqueness / timeliness is controlled by generating and checking time stamps or sequence numbers (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 3.

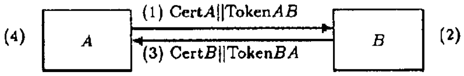


Figure 3

The form of the token (TokenAB), sent by A to B, is identical to that specified in 5.1.1.

$$\text{Token}AB = {}^{T_A}_{N_A}||B||\text{Text2}||sS_A\left({}^{T_A}_{N_A}||B||\text{Text1}\right).$$

The form of the token (TokenBA), sent by B to A, is:

$$\text{Token}BA = {}^{T_B}_{N_B}||A||\text{Text4}||sS_B\left({}^{T_B}_{N_B}||A||\text{Text3}\right).$$

The choice of using either time stamps or sequence numbers in this mechanism depends on the technical capabilities of the claimant and the verifier as well as on the environment.

NOTE 1 — The inclusion of identifiers A and B in the signed data of TokenBA and TokenAB, respectively, is necessary to prevent the tokens from being accepted by anyone other than the intended verifier.

Steps (1) and (2) are identical to those specified in 5.1.1, one pass authentication.

(3) B sends TokenBA and, optionally, its certificate to A.

(4) The message in step (3) is handled in a manner analogous to step (2) of 5.1.1.

NOTE 2 — The two messages of this mechanism are not bound together in any way, other than implicitly by timeliness; the mechanism involves independent use of mechanism 5.1.1 twice. Further binding together of these messages can be achieved by making appropriate use of the text fields.

5.2.2 Three pass authentication

In this authentication mechanism uniqueness / timeliness is controlled by generating and checking random numbers (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 4.

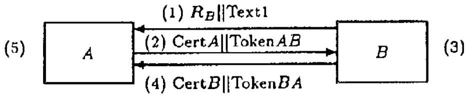


Figure 4

The tokens are of the following form:

$$\text{Token}AB = R_A||R_B||B||\text{Text3}||sS_A\,(R_A||R_B||B||\text{Text2}),$$
$$\text{Token}BA = R_B||R_A||A||\text{Text5}||sS_B\,(R_B||R_A||A||\text{Text4}).$$

The inclusion of the parameter B in TokenAB and the inclusion of the parameter A in TokenBA are optional. They depend on the environment in which this authentication mechanism is used.

NOTE — The inclusion of the random number R_A in the signed part of TokenAB prevents B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This measure may be required, for example, when the same key is used by A for purposes other than entity authentication. However, the inclusion of R_B in TokenBA, whilst necessary for security reasons which dictate that A should check that it is the same as the value sent in the first message, may not offer the same protection to B, since R_B is known to A before R_A is chosen. If this type of protection is required, B can insert an additional random number R'_B in the text fields Text4 and Text5 of TokenBA.

(1) B sends a random number R_B and, optionally, a text field Text1 to A.

(2) A sends TokenAB and, optionally, its certificate to B.

(3) On receipt of the message containing TokenAB, B performs the following steps:

  (i) It ensures that it is in possession of a valid public key of A either by verifying the certificate of A or by some other means.

  (ii) It verifies TokenAB by checking the signature of A contained in the token, by checking that the random number R_B, sent to A in step (1), agrees with the random number contained in the signed data of TokenAB, and by checking that the value of the identifier field (B) in the signed data of TokenAB, if present, is equal to B's distinguishing identifier.

(4) B sends TokenBA and, optionally, its certificate to A.

(5) On receipt of the message containing TokenBA, A analogously performs steps (i) and (ii) listed under (3). In addition, A checks that the random number R_B contained in the signed data of TokenBA is equal to the random number R_B received in step (1).

5.2.3 Two pass parallel authentication

In this mechanism authentication is carried out in parallel. Uniqueness / timeliness is controlled by generating and checking random numbers (see Annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 5.

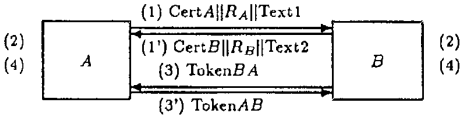


Figure 5

The tokens are similar to those of clause 5.1.2:

$$\text{Token}AB = R_A||R_B||B||\text{Text4}||sS_A\,(R_A||R_B||B||\text{Text3}),$$
$$\text{Token}BA = R_B||R_A||A||\text{Text6}||sS_B\,(R_B||R_A||A||\text{Text5}).$$

The inclusion of the parameter B in TokenAB and the inclusion of the parameter A in TokenBA are optional. They depend on the environment in which this authentication mechanism is used.

NOTE 1 — The random number R_A is present in TokenAB to prevent B from obtaining the signature of A on data chosen by B prior to the start of the authentication mechanism. This prevention may be required, for example, when the same key is used by A for other purposes in addition to entity authentication. For similar reasons the random number R_B is present in TokenBA. Depending on the relative time of receipt of the messages sent in steps (1) and (1'), one of the parties may know the random number of the other party when choosing its random number. If this is undesirable, both parties can insert an additional random number R'_A and R'_B in the text fields Text3 and Text4 of TokenAB, and Text5 and Text 6 of TokenBA, respectively.

(1) A sends R_A and, optionally, its certificate and a text field Text1 to B.

(1') B sends R_B and, optionally, its certificate and a text field Text2 to A.

(2) A and B ensure that they are in possession of a valid public key of the other entity either by verifying the respective certificate or by some other means.

(3) A sends TokenAB to B.

(3') B sends TokenBA to A.

(4) A and B perform the following steps:

Each of them verifies the received token by checking the signature contained in the token and by checking that the random number, which it previously sent to the other entity, agrees with the random number contained in the signed data of the token received.

NOTE 2 — An alternative to mechanism 5.2.3 is to run mechanism 5.1.2 both ways. The inclusion of the certificates in the first messages of mechanism 5.2.3 allows for earlier certificate verification which may speed up the authentication process.

Annex A
(informative)

Use of text fields

The tokens specified in clause 5 of this part of ISO/IEC 9798 contain text fields. The actual use of and the relationships between the various text fields in a given pass depend on the application. Some examples are given below; see also Annex A of ISO/IEC 9798-1.

If a signature scheme without message recovery is used and if the signed text field is not empty, then the verifier needs to be in possession of the text prior to verifying the signature. In this Annex "signed text fields" refers to text fields in the signed data and "unsigned text fields" refers to text fields in the unsigned data.

For example, if a digital signature scheme without message recovery is used, any information requiring data origin authentication should be placed in the signed text field and (as part of) the unsigned text field in the token.

If the tokens do not contain (sufficient) redundancy, the signed text fields may be used to provide additional redundancy.

Signed text fields may be used to indicate that the token is only valid for the purpose of entity authentication. Should there be a concern that one entity might choose a "degenerate" value with malicious intent for the other entity to sign, the other entity may introduce a random number in the text field.

Should an algorithm be used where it may be possible to launch attacks based on the fact that a particular claimant is using the same key for all verifiers with which the claimant communicates, and if such attacks are considered to be a threat, the identity of the intended verifier should be included in the signed text field and, if necessary, in the unsigned text field.

Unsigned text fields can also be used to provide information to a verifier indicating the (unauthenticated) identity which a claimant is claiming. If means other than certificates are used for distributing public keys, such information may be required to allow a verifier to determine which public key is to be used to authenticate a claimant.

ICS 35.040

Descriptors: data processing, information interchange, data transmission, protection of information, security techniques, coding (data conversion), authentication, message authentication codes, algorithms.

Price based on 6 pages

INTERNATIONAL STANDARD

ISO/IEC 9798-4

Second edition
1999-12-15

Information technology — Security techniques — Entity authentication —

Part 4: Mechanisms using a cryptographic check function

Technologies de l'information — Techniques de sécurité — Authentification d'entité —

Partie 4: Mécanismes utilisant une fonction cryptographique de vérification

Reference number
ISO/IEC 9798-4:1999(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 9798 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 9798-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques.*

This second edition cancels and replaces the first edition (ISO/IEC 9798-4:1995), which has been technically revised. Note, however, that implementations which comply with ISO/IEC 9798-4 (1st edition) will be compliant with ISO/IEC 9798-4 (2nd edition).

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication*:

— *Part 1: General*

— *Part 2: Mechanisms using symmetric encipherment algorithms*

— *Part 3: Mechanisms using digital signature techniques*

— *Part 4: Mechanisms using a cryptographic check function*

— *Part 5: Mechanisms using zero knowledge techniques*

Further parts may follow.

Annex A of this part of ISO/IEC 9798 is for information only.

Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function

1 Scope

This part of ISO/IEC 9798 specifies entity authentication mechanisms using a cryptographic check function. Two mechanisms are concerned with the authentication of a single entity (unilateral authentication), while the remaining are mechanisms for mutual authentication of two entities.

The mechanisms specified in this part of ISO/IEC 9798 use time variant parameters such as time stamps, sequence numbers, or random numbers, to prevent valid authentication information from being accepted at a later time or more than once.

If a time stamp or sequence number is used, one pass is needed for unilateral authentication, while two passes are needed to achieve mutual authentication. If a challenge and response method employing random numbers is used, two passes are needed for unilateral authentication, while three passes are required to achieve mutual authentication.

Examples of cryptographic check functions are given in ISO/IEC 9797.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 9798 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs).*

ISO/IEC 9798-1:1997, *Information technology — Security techniques — Entity authentication — Part 1: General.*

3 Definitions and notation

For the purposes of this part of ISO/IEC 9798, the definitions and notation described in ISO/IEC 9798-1 apply.

4 Requirements

In the authentication mechanisms specified in this part of ISO/IEC 9798 an entity to be authenticated corroborates its identity by demonstrating its knowledge of a secret authentication key. This is achieved by the entity using its secret key with a cryptographic check function applied to specific data to obtain a cryptographic check value. The cryptographic check value can be checked by anyone sharing the entity's secret authentication key, who can re-calculate the cryptographic check value and compare it with the value received.

The authentication mechanisms have the following requirements. If any one of these is not met then the authentication process may be compromised or it cannot be implemented.

a) A claimant authenticating itself to a verifier shares a common secret authentication key with that verifier. This key shall be known to the involved parties prior to the commencement of any particular run of an authentication mechanism. The method by which the key is distributed to the entities is beyond the scope of this part of ISO/IEC 9798.

b) The secret authentication key shared by a claimant and a verifier shall be known only to those two entities and, possibly, to other parties they both trust.

c) The strength of the mechanisms is dependent on the length and the secrecy of the key, on the nature of the cryptographic check functions, and on the length of the check value. These parameters shall be chosen to meet the required security level, as may be specified by the security policy.

5 Mechanisms

In these authentication mechanisms the entities A and B shall share a common secret authentication key K_{AB} or two unidirectional secret keys K_{AB} and K_{BA} prior to the commencement of any particular run of the authentication mechanisms. In the latter case, the unidirectional keys K_{AB} and K_{BA} are used respectively for the authentication of A by B and of B by A.

The mechanisms require the use of time variant parameters such as time stamps, sequence numbers or random numbers. The properties of the time variant parameters are important for the security of these mechanisms. In particular, the parameters shall be chosen so that it shall be most unlikely for them to repeat within the lifetime of an authentication key. For additional information see annex B of ISO/IEC 9798-1.

The use of the text fields specified in the following mechanisms is outside the scope of this part of ISO/IEC 9798 (they may be empty), and will depend upon the specific application. See annex A for information on the use of text fields.

A text field may only be included in the input to the cryptographic check function if the verifier can determine it independently, e.g., if it is known in advance, sent in clear or can be derived from one or both of those sources.

5.1 Unilateral authentication

Unilateral authentication means that only one of the two entities is authenticated by use of the mechanism.

5.1.1 One pass authentication

In this authentication mechanism the claimant A initiates the process and is authenticated by the verifier B. Uniqueness/timeliness is controlled by generating and checking a time stamp or a sequence number (see annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 1.

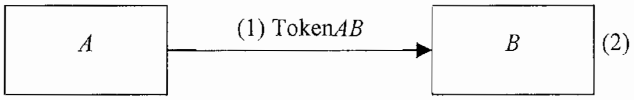


Figure 1

The form of the token ($\text{Token}AB$), sent by the claimant A to the verifier B is:

$$\text{Token}AB = \genfrac{}{}{0pt}{}{T_A}{N_A} \,||\, \text{Text2} \,||\, f_{K_{AB}}(\genfrac{}{}{0pt}{}{T_A}{N_A} \,||\, B \,||\, \text{Text1})$$

where the claimant A uses either a sequence number N_A or a time stamp T_A as the time variant parameter. The choice depends on the technical capabilities of the claimant and the verifier as well as on the environment. As defined in ISO/IEC 9798-1, $f_K(X)$ denotes the cryptographic check value computed by applying the cryptographic check function f to the data X using the key K.

The inclusion of the distinguishing identifier B in TokenAB is optional.

NOTE Distinguishing identifier B is included in TokenAB to prevent the re-use of TokenAB on entity A by an adversary masquerading as entity B. Its inclusion is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier B may also be omitted if a unidirectional key is used.

(1) A generates and sends TokenAB to B.

(2) On receipt of the message containing TokenAB, B verifies TokenAB by checking the time stamp or the sequence number, calculating

$$f_{K_{AB}}(\begin{smallmatrix} T_A \\ N_A \end{smallmatrix} \| B \| \text{Text1})$$

and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, as well as the time stamp or the sequence number.

5.1.2 Two pass authentication

In this authentication mechanism the claimant A is authenticated by the verifier B who initiates the process. Uniqueness/timeliness is controlled by generating and checking a random number R_B (see annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 2.

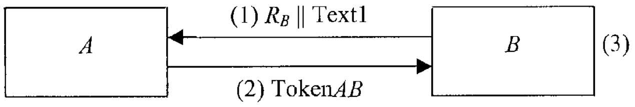


Figure 2

The form of the token (TokenAB), sent by the claimant A to the verifier B is:

$$\text{Token}AB = \text{Text3} \| f_{K_{AB}}(R_B \| B \| \text{Text2})\,.$$

The inclusion of the distinguishing identifier B in TokenAB is optional.

NOTE Distinguishing identifier B is included in TokenAB to prevent a so-called reflection attack. Such an attack is characterised by the fact that an intruder 'reflects' the challenge R_B to B pretending to be A. The inclusion of the distinguishing identifier B is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier B may also be omitted if a unidirectional key is used.

(1) B generates a random number R_B and sends it and, optionally, a text field Text1 to A.

(2) A generates and sends TokenAB to B.

(3) On receipt of the message containing TokenAB, B verifies TokenAB by calculating

$$f_{K_{AB}}(R_B \,||\, B \,||\, \text{Text2})$$

and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, and that the random number R_B, sent to A in step (1), was used in constructing TokenAB.

5.2 Mutual authentication

Mutual authentication means that the two communicating entities are authenticated to each other by use of the mechanism.

The two mechanisms described in 5.1.1 and 5.1.2 are adapted in 5.2.1 and 5.2.2, respectively, to achieve mutual authentication. In both cases this requires one more pass and results in two more steps.

NOTE A third mechanism for mutual authentication can be constructed from two instances of the mechanism specified in 5.1.2, one started by entity A and the other by entity B.

5.2.1 Two pass authentication

In this authentication mechanism uniqueness/timeliness is controlled by generating and checking time stamps or sequence numbers (see annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 3.

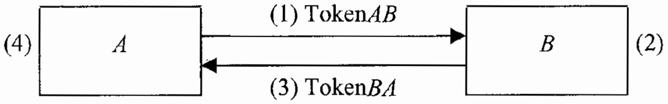


Figure 3

The form of the token (TokenAB), sent by A to B, is identical to that specified in 5.1.1.

$$\text{Token}AB = \genfrac{}{}{0pt}{}{T_A}{N_A} \,||\, \text{Text2} \,||\, f_{K_{AB}}(\genfrac{}{}{0pt}{}{T_A}{N_A} \,||\, B \,||\, \text{Text1}).$$

The form of the token (TokenBA), sent by B to A, is:

$$\text{Token}BA = \genfrac{}{}{0pt}{}{T_B}{N_B} \,||\, \text{Text4} \,||\, f_{K_{AB}}(\genfrac{}{}{0pt}{}{T_B}{N_B} \,||\, A \,||\, \text{Text3}).$$

The inclusion of the distinguishing identifier B in TokenAB and the inclusion of the distinguishing identifier A in TokenBA are (independently) optional.

NOTE 1 Distinguishing identifier B is included in TokenAB to prevent the re-use of TokenAB on entity A by an adversary masquerading as entity B. For similar reasons the distinguishing identifier A is present in TokenBA. Their inclusion is made optional so that, in environments where such attacks cannot occur, one or both may be omitted.

The distinguishing identifiers A and B may also be omitted if unidirectional keys (see below) are used.

The choice of using either time stamps or sequence numbers in this mechanism depends on the capabilities of the claimant and the verifier as well as on the environment.

Steps (1) and (2) are identical to those specified in 5.1.1, one pass authentication.

(3) B generates and sends TokenBA to A.

(4) The message in step (3) is handled in a manner analogous to step (2) of 5.1.1.

NOTE 2 The two messages of this mechanism are not bound together in any way, other than implicitly by timeliness; the mechanism involves independent use of mechanism 5.1.1 twice. Further binding together of these messages can be achieved by making appropriate use of the text fields (see annex A).

If unidirectional keys are used then the key K_{AB} in TokenBA is replaced by the unidirectional key K_{BA}, and the appropriate key is used in step (4).

5.2.2 Three pass authentication

In this authentication mechanism uniqueness/timeliness is controlled by generating and checking random numbers (see annex B of ISO/IEC 9798-1).

The authentication mechanism is illustrated in figure 4.

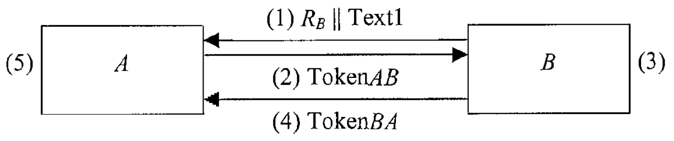


Figure 4

The tokens are of the following form:

$$\text{Token}AB = R_A \,||\, \text{Text3} \,||\, f_{K_{AB}}(R_A \,||\, R_B \,||\, B \,||\, \text{Text2}),$$

$$\text{Token}BA = \text{Text5} \,||\, f_{K_{AB}}(R_B \,||\, R_A \,||\, \text{Text4}).$$

The inclusion of the distinguishing identifier B in TokenAB is optional.

NOTE When present, distinguishing identifier B is included in TokenAB to prevent a so-called reflection attack. Such an attack is characterised by the fact that an intruder 'reflects' the challenge R_B to B pretending to be A. The inclusion of the distinguishing identifier B is made optional so that, in environments where such attacks cannot occur, it may be omitted.

The distinguishing identifier B may also be omitted if unidirectional keys (see below) are used.

(1) B generates a random number R_B and sends it and, optionally, a text field Text1 to A.

(2) A generates a random number R_A, and generates and sends TokenAB to B.

(3) On receipt of the message containing TokenAB, B verifies TokenAB by calculating

$$f_{K_{AB}}(R_A \,||\, R_B \,||\, B \,||\, \text{Text2})$$

and comparing it with the cryptographic check value of the token, thereby verifying the correctness of the distinguishing identifier B, if present, and that the random number R_B, sent to A in step (1), was used in constructing TokenAB.

(4) B generates and sends TokenBA to A.

(5) On receipt of the message containing TokenBA, A verifies TokenBA by calculating

$$f_{K_{AB}}(R_B \,||\, R_A \,||\, \text{Text4})$$

and comparing it with the cryptographic check value of the token, thereby verifying that the random number R_B, received from B in step (1), was used in constructing TokenBA and that the random number R_A, sent to B in step (2), was used in constructing TokenBA.

If unidirectional keys are used then the key K_{AB} in TokenBA is replaced by the unidirectional key K_{BA} and the appropriate key is used in step (5).

Annex A
(informative)

Use of text fields

The tokens specified in clause 5 of this part of ISO/IEC 9798 contain text fields. The actual use of and the relationships between the various text fields in a given pass depend on the application.

For example, through its inclusion in an appropriate text field, e.g. Text1 of Token*AB* in clause 5.1.1, information can be used in the calculation of the cryptographic check value of the token. By this means, data origin authentication can be provided for this information.

See Annex A of ISO/IEC 9798-1 for further examples of the use of text fields.

ICS 35.040
Price based on 7 pages

INTERNATIONAL STANDARD

ISO/IEC 9798-5

First edition
1999-03-15

Information technology — Security techniques — Entity authentication —

Part 5:
Mechanisms using zero knowledge techniques

Technologies de l'information — Techniques de sécurité — Authentification d'entité —

Partie 5: Mécanismes utilisant les techniques de connaissance du zéro

Reference number
ISO/IEC 9798-5:1999(E)

Contents

ISO/IEC Copyright Office • Case Postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

International Standard ISO/IEC 9798-5 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Sub-Committee SC27, *IT Security techniques.*

ISO/IEC 9798 consists of the following parts, under the general title *Information technology — Security techniques — Entity authentication*:

- *Part 1: General*
- *Part 2: Mechanisms using symmetric encipherment algorithms*
- *Part 3: Mechanisms using digital signature techniques*
- *Part 4: Mechanisms using a cryptographic check function*
- *Part 5: Mechanisms using zero knowledge techniques*

Annexes A, B, C, D, E, and F of this part of ISO/IEC 9798 are for information only.

ISO and IEC draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 9798 may involve the use of patents as given in Annex E.

ISO and IEC take no position regarding the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from the addresses given in Annex E.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 9798 may be the subject of patent rights other than those identified in Annex E. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero knowledge techniques

1 Scope

This part of ISO/IEC 9798 specifies three entity authentication mechanisms using zero knowledge techniques. All the mechanisms specified in this part of ISO/IEC 9798 provide unilateral authentication. These mechanisms are constructed using the principles of zero knowledge, but they will not be zero knowledge according to the strict definition sketched in Annex A for all choices of parameters.

The first mechanism is said to be based on identities. A trusted accreditation authority provides each claimant with private accreditation information, computed as a function of the claimant's identification data and the accreditation authority's private key.

The second mechanism is said to be certificate-based using discrete logarithms. Every claimant possesses a public key, private key pair for use in this mechanism. Every verifier of a claimant's identity must possess a trusted copy of the claimant's public verification key; the means by which this is achieved is beyond the scope of this standard, but it may be achieved through the distribution of certificates signed by a Trusted Third Party.

The third mechanism is said to be certificate-based using an asymmetric encipherment system. Every claimant possesses a public key, private key pair for an asymmetric cryptosystem. Every verifier of a claimant's identity must possess a trusted copy of the claimant's public key; the means by which this is achieved is beyond the scope of this standard, but it may be achieved through the distribution of certificates signed by a Trusted Third Party.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 9798. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 9796: 1991, *Information technology — Security techniques — Digital signature scheme giving message recovery.*

ISO/IEC 9798-1, *Information technology — Security techniques — Entity authentication mechanisms — Part 1: General.*

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions.*

3 Definitions

For the purposes of this part of ISO/IEC 9798, the following definitions apply.

The following terms are defined in ISO/IEC 9798-1.

3.1 asymmetric cryptographic technique:

3.2 asymmetric encipherment system:

3.3 asymmetric key pair:

3.4 challenge:

3.5 claimant:

3.6 decipherment:

3.7 distinguishing identifier:

3.8 encipherment:

3.9 entity authentication:

3.10 private key:

3.11 public key:

3.12 public verification key:

3.13 random number:

3.14 token:

3.15 trusted third party:

3.16 unilateral authentication:

3.17 verifier:

The following term is defined in ISO/IEC 10118-1.

3.18 hash-function: function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

- it is computationally infeasible to find for a given output an input which maps to this output;
- it is computationally infeasible to find for a given input a second input which maps to the same output.

In addition the following definitions are used.

3.19 accreditation authority: entity trusted by all members of a group of entities for the purposes of the generation of private accreditation information.

3.20 accreditation multiplicity parameter: positive integer equal to the number of items of secret accreditation information provided to an entity by the accreditation authority.

3.21 exchange multiplicity parameter: positive integer used to determine how many times the exchange of entity authentication messages shall be performed in one instance of the authentication mechanism.

3.22 identification data: sequence of data items, including the distinguishing identifier for an entity, assigned to an entity and used to identify it.

NOTE — Examples of data items which may be included in the identification data include: an account number, expiry date, serial number, etc.

3.23 private accreditation exponent: value known only to the accreditation authority, and which is used in the production of claimants' private accreditation information. This value shall be kept secret. This value is related to the public accreditation verification exponent.

3.24 private accreditation information: private information provided to a claimant by an accreditation authority, and of which a claimant subsequently proves knowledge, thereby establishing the claimant's identity.

3.25 private decipherment transformation: decipherment transformation determined by an asymmetric encipherment system and the private key of an asymmetric key pair.

3.26 public accreditation verification exponent: value agreed by all members of a group of entities, and which, in conjunction with the modulus, determines the value of the private accreditation exponent.

3.27 public encipherment transformation: encipherment transformation determined by an asymmetric encipherment system and the public key of an asymmetric key pair.

3.28 redundant identity: sequence of data items obtained from an entity's identification data by adding redundancy using techniques specified in ISO/IEC 9796.

3.29 response: data item sent by the claimant to the verifier, and which the verifier can process to help check the identity of the claimant.

3.30 witness: data item which provides evidence of the claimant's identity to the verifier.

4 Symbols and notation

For the purposes of this part of ISO/IEC 9798 the following symbols and notation described in ISO/IEC 9798-1 apply.

A — The distinguishing identifier of entity A.

B — The distinguishing identifier of entity B.

$Y||Z$ — The result of the concatenation of the data items Y and Z in that order.

The following general symbols and notation are used.

d — A challenge.

D — A response.

h — A hash-function.

r — A random number.

$\lfloor x \rfloor$ — The largest integer which is not greater than the value x.

mod — If i is an integer and n is a positive integer, then $i \bmod n$ denotes the unique integer j which satisfies

a) $0 \leq j < n$, and

b) $i - j$ is an integer multiple of n.

In the context of the identity-based mechanism of clause 5, the following symbols and notation are used.

$C_{A1}, C_{A2}, \ldots, C_{Am}$ — Entity A's private accreditation information.

gcd — The greatest common divisor of two integers, i.e. $\gcd(a,b)$ represents the largest positive integer that is a divisor of both a and b.

$I_{A1}, I_{A2}, \ldots, I_{Am}$ — The identification data of entity A. I_{Ai} is the ith part of the identification data of entity A.

$J_{A1}, J_{A2}, \ldots, J_{Am}$ — The redundant identity of entity A. J_{Ai} is the ith part of the redundant identity of entity A.

k_s — An integer determined by the modulus n, and which determines the maximum bit-length of the parts of an entity's redundant identity.

lcm — The least common multiple of two integers, i.e. $\mathrm{lcm}(a,b)$ represents the smallest positive integer that is a multiple of both a and b.

m — The accreditation multiplicity parameter.

n — A modulus equal to the product of the prime numbers p and q.

p — A prime number used to calculate the modulus.

q — A prime number used to calculate the modulus.

t — The exchange multiplicity parameter.

u — The accreditation authority's private accreditation exponent.

v — The public accreditation verification exponent.

W — A witness.

mod* — If i is an integer and n is a positive integer, then $i \bmod^* n$ denotes the non-negative integer j equal to the smaller of the two values: $i \bmod n$ and $n - i \bmod n$. If i and j are two integers and n is a positive integer then $i \equiv j \pmod{^*n}$ if and only if $i \bmod^* n = j \bmod^* n$.

$(a|n)$ — The Jacobi symbol of the positive integer a with respect to the odd positive integer n.

NOTE — Let p be an odd prime and let a be a positive integer. The Legendre symbol of a with respect to p, written $(a|p)$, is defined by

$$(a|p) = a^{(p-1)/2} \bmod p.$$

When a is not a multiple of p, $(a|p)$ is either +1 or -1, depending on whether or not a is equal to the square of an integer modulo p. The Legendre symbol of multiples of p with respect to a prime p is zero.

Let n be an odd positive integer satisfying $n = pq$, where p and q are primes, and let a be a positive integer. The Jacobi symbol of a with respect to n, written $(a|n)$, is defined by

$$(a|n) = (a|p)(a|q).$$

The Jacobi symbol $(a|n)$ can be computed efficiently without knowledge of the prime factorisation of n, see [6] and [8].

In the context of the discrete logarithm based mechanism of clause 6, the following symbols and notation are used.

g — A positive integer which is the base of the discrete logarithms.

p — A prime number used as a modulus.

q — A prime number which is a factor of $p-1$.

y_X — The public verification key for entity X.

z_X — The private authentication key for entity X.

In the context of the trusted public transformation based mechanism of clause 7, the following symbols and notation are used.

P_X — The public encipherment transformation for entity X.

S_X — The private decipherment transformation for entity X.

5 Mechanism based on identities

In this clause an entity authentication mechanism is specified which is based on the use of identities.

5.1 Specific requirements

In order to use the mechanism within a group of entities, the following steps shall be taken.

a) Every entity wishing to act as either a claimant or a verifier must have the means to generate random numbers.

b) An accreditation authority shall be appointed for the group of entities. This accreditation authority shall be trusted by all members of the group for the purposes of guaranteeing identities.

c) A number of parameters shall be selected, which will govern the operation of the entity authentication mechanism. The selected parameters shall be made known in a reliable manner to all members of the group of entities.

d) Every entity wishing to act as a claimant in the authentication mechanism must be provided with identification data by some means. In this context identification data is a string of bits of length limited by one of the parameters selected in step (c), and which uniquely and meaningfully identifies the entity according to an agreed convention.

e) Every entity wishing to act as a claimant in the authentication mechanism shall be issued with private accreditation information by the selected accreditation authority.

f) If the version of the mechanism using a hash-function is selected, all entities within the group must agree on the use of a specific hash-function (for example one of the functions specified in ISO/IEC 10118).

5.2 Parameter selection

The parameters to be selected are as follows.

a) The public accreditation verification exponent v. Certain values, such as 2, 3 and $2^{16}+1 = 65537$, have some practical advantages.

b) The modulus n. This positive integer shall be selected by the appointed accreditation authority. The value of n shall be equal to the product of two prime numbers p and q. The values of p and q shall be kept secret by the accreditation authority. The prime numbers p and q shall be chosen in such a way that knowledge of their product n shall not feasibly enable any entity to deduce them, where feasibility is defined by the context of use of the authentication mechanism.

The values of p and q shall satisfy the following constraints:

— if v is odd, then $\gcd(p-1, v) = \gcd(q-1, v) = 1$, and

— if v is even, then $\gcd((p-1)/2, v) = \gcd((q-1)/2, v) = 1$, and $p-q$ shall not be a multiple of 8.

The choice of n determines the value of a further parameter, which is denoted by k_s, in the following way:

$$k_s = \lfloor \log_2(n) \rfloor .$$

In other words, a binary representation of n shall contain $k_s + 1$ bits.

The choice of n also determines the value of the accreditation authority's private accreditation exponent, denoted u, in the following way. The value u shall be set to the least positive integer such that $uv+1$ is a multiple of

$$\begin{array}{ll} \mathrm{lcm}(p-1, q-1) & \text{if } v \text{ is odd}, \\ \mathrm{lcm}(p-1, q-1)/2 & \text{if } v \text{ is even}. \end{array}$$

c) The accreditation multiplicity parameter m. This positive integer shall be chosen in conjunction with the public accreditation verification exponent v and the exchange multiplicity t, and affects the level of security of the scheme.

d) The exchange multiplicity parameter t. This positive integer shall be chosen in conjunction with the public accreditation verification exponent v and the accreditation multiplicity m, and affects the level of security of the scheme.

NOTE 1 — Guidance on the choice of parameters for this mechanism is given in Annex B.

NOTE 2 — When $v = 2$ the mechanism becomes the Fiat-Shamir scheme, [3]. When $v > 2$, $m = 1$, and v is a prime the mechanism becomes the Guillou-Quisquater scheme, [5].

5.3 Identity selection

Each entity wishing to act as a claimant in this mechanism must be assigned identification data consisting of a sequence of m parts: $I_{A1}, I_{A2}, \ldots, I_{Am}$. Each part of the identification data shall contain at most $8\lfloor (k_s+3)/16 \rfloor$ bits.

The entity authentication mechanism will provide assurance to the verifier that the claimant is the entity which has been assigned this identification data.

NOTE 1 — This sequence of identification data parts could, for example, be constructed by assigning an entity a single identifying string of bits, and appending the binary representations of the numbers $1, 2, \ldots, m$ in turn to this string to obtain the values $I_{A1}, I_{A2}, \ldots, I_{Am}$. In such an approach, the binary representations of the numbers $1, 2, \ldots, m$ could conveniently all be made of the same length, by prefixing with zeros as necessary.

NOTE 2 — If the parts of an entity's identification data are longer than the maximum permissible length, then this can be dealt with by applying a hash-function to the identification data parts to obtain the values $I_{A1}, I_{A2}, \ldots, I_{Am}$. Examples of hash-functions can be found in ISO/IEC 10118.

NOTE 3 — Expiry of an entity's identification data can be enforced by the inclusion of an expiry date in the identification data. Revocation of an entity's identification data can be simplified by the inclusion of a serial number in the identification data.

5.4 Accreditation generation

To generate the private accreditation information for an entity A, the accreditation authority shall compute a sequence of m digital signatures $C_{A1}, C_{A2}, \ldots, C_{Am}$. More specifically, for every i $(1 \leq i \leq m)$, C_{Ai} shall be computed using the following procedure.

a) J_{Ai}, the ith part of the 'redundant identity' for A, shall be computed from I_{Ai}, the ith part of the identification data of A, by subjecting I_{Ai} to the first four steps of the signature process specified in ISO/IEC 9796, ('Padding', 'Extension', 'Redundancy' and 'Truncation and forcing'), using the specified value of k_s. The value obtained from this process, denoted IR, shall then be used to derive J_{Ai} in the following way.

— If v is odd then $J_{Ai} = IR$.

— If v is even and if $(IR|n) = +1$ then $J_{Ai} = IR$.

— If v is even and if $(IR|n) = -1$ then $J_{Ai} = IR/2$.

b) C_{Ai} shall be computed from J_{Ai} using the following formula:

$$C_{Ai} = (J_{Ai})^u \ \mathrm{mod}^* n.$$

The private accreditation information supplied to entity A is equal to the computed signatures $C_{A1}, C_{A2}, \ldots, C_{Am}$.

Observe that

$$(C_{Ai})^v J_{Ai} \equiv 1 \ (\mathrm{mod}^* n)$$

for every i $(1 \leq i \leq m)$.

5.5 Authentication exchange

This unilateral authentication mechanism involves the following exchanges of information between a claimant A and a verifier B, and enables B to check the identity of A. It is necessary for correct operation of the mechanism that B is provided with the claimed identification data of A, either appended to one of the information exchanges in the mechanism or by some other means.

One iteration of the authentication procedure is illustrated in figure 1. The bracketed numbers in the figure correspond to the steps of the exchange described in detail below.

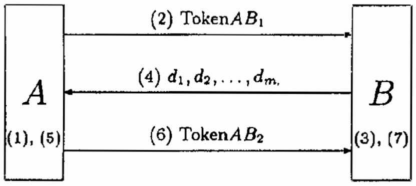


Figure 1 — Identity-based mechanism

The form of the first token (TokenAB_1), sent by the claimant to the verifier is either:

$$\text{Token}AB_1 = W$$

or

$$\text{Token}AB_1 = h(W||\text{Text})$$

where W is the witness, h is a hash-function, and Text is an optional text field. This text field is available for use in applications outside the scope of this part of ISO/IEC 9798 (it may be empty). See annex A of ISO/IEC 9798-1 for information on the use of text fields. If this text field is non-empty then B must have the means to recover the value of the text field; this may require A to send all or part of the text field with TokenAB_1 (see also Note 1 below).

The form of the second token (TokenAB_2), sent by the claimant to the verifier is:

$$\text{Token}AB_2 = D$$

where D is the response.

For each application of this mechanism the following authentication procedure shall be performed t times (where t is the exchange multiplicity parameter). The verifier B shall only accept the claimant A as valid if all t iterations of the procedure complete successfully.

(1) Entity A, who is equipped with private accreditation information $C_{A1}, C_{A2}, \ldots, C_{Am}$, chooses a random number r, subject to the restriction that r shall be an integer satisfying $1 \leq r \leq n - 1$. This integer is kept secret by A. A now computes the witness W as

$$W = r^v \bmod^* n.$$

(2) A sends TokenAB_1 to B. TokenAB_1 shall be equal to either W or $h(W||\text{Text})$.

(3) Having received TokenAB_1, B shall choose at random a sequence of integers $d_1, d_2, \ldots, d_m$, where each value d_i shall lie in the range 0 to $v - 1$. This sequence of integers is the challenge.

(4) B sends the challenge $d_1, d_2, \ldots, d_m$ to A.

(5) On receipt of the challenge $d_1, d_2, \ldots, d_m$, A shall compute the response D from the (secret) value r and the private accreditation information $C_{A1}, C_{A2}, \ldots, C_{Am}$ as follows:

$$D = r \prod_{i=1}^{m} (C_{Ai})^{d_i} \bmod^* n.$$

(6) A sends Token$AB_2 = D$ to B.

(7) On receipt of the response D, B shall perform the following computations.

(a) B checks that $0 < D < n/2$. If not then B shall reject A.

(b) B calculates $J_{A1}, J_{A2}, \ldots, J_{Am}$, the redundant identity of A, from the identification data $I_{A1}, I_{A2}, \ldots, I_{Am}$ of A, using the same process as specified in clause 5.4, step (a).

(c) B now computes the value W' using the following formula:

$$W' = D^v \prod_{i=1}^{m} (J_{Ai})^{d_i} \bmod^* n.$$

(d) If W was sent in the first exchange of the procedure then B checks that the computed value W' is equal to the value of W sent in the first exchange of the procedure. Alternatively, if $h(W||\text{Text})$ was sent in the first exchange of the procedure then B first computes $h(W'||\text{Text})$ and then checks that $h(W'||\text{Text})$ is equal to the value of $h(W||\text{Text})$ sent in the first exchange of the procedure. If the check succeeds then this iteration of the mechanism is successful. Otherwise B rejects A.

NOTE 1 — Other information may be sent with any of the exchanges of any of the iterations of the authentication procedure. In particular note that information included within the identification data of A may be sent with TokenAB_1 in the first exchange of the first of the t iterations of the authentication procedure (step (2)). Such information might be used by B to help compute A's redundant identity and/or the value of the optional Text field.

NOTE 2 — It is important that A chooses the random value r by a process which guarantees that selected values are independent within the lifetime of the accreditation information. If, for example, the same value r is used twice, then a third party may be able to deduce part or all of the private accreditation information of A, and hence be able to impersonate A successfully.

NOTE 3 — The redundant identity $J_{A1}, J_{A2}, \ldots, J_{Am}$ for A can be computed at any stage by B, i.e. B need not wait until the receipt of the response D before computing $J_{A1}, J_{A2}, \ldots, J_{Am}$. If B verifies A frequently using this mechanism, then B may cache the values $J_{A1}, J_{A2}, \ldots, J_{Am}$.

NOTE 4 — The t iterations of the procedure can be performed in parallel, i.e. in the first step A may choose t random numbers $r_1, r_2, \ldots, r_t$, compute t witnesses $W_1, W_2, \ldots, W_t$, send them simultaneously to B, and so on. If this 'parallel implementation' is adopted, the total number of message exchanges will be equal to three, regardless of the value of t.

NOTE 5 — The use of $h(W||\text{Text})$ instead of W in the first exchange of the procedure can achieve efficiency gains by reducing the number of bits in TokenAB_1.

NOTE 6 — It is recommended that the private accreditation information used in this mechanism be used only for the purposes of authentication, and should not be used for any other application (e.g. generation of digital signatures). If this recommendation is not followed then special care should be taken to prevent the verifier using the claimant as a 'signing oracle'; this could, for example, be achieved by requiring the challenge to be of a specially chosen form.

6 Certificate-based mechanism using discrete logarithms

In this clause an entity authentication mechanism is specified which uses discrete logarithms.

NOTE — This mechanism is known as the Schnorr scheme, [10].

6.1 Specific requirements

In order to use the mechanism within a group of entities, the following steps shall be taken.

a) Every entity wishing to act as either a claimant or a verifier must have the means to generate random numbers.

b) All entities within the group must agree on three positive integers p, q and g. The integer p must be chosen to be a prime number. Further q must be chosen to be a prime number which is also a factor of $p - 1$. Finally g must be chosen to be an element of order q modulo p, that is g must satisfy:

(i) $g^q \bmod p = 1$, and

(ii) $g \neq 1$.

The values p and g should be chosen so that, given an arbitrary integer i $(1 < i < q)$, finding an integer j (if one exists) such that $g^j \bmod p = i$ shall be computationally infeasible.

c) All entities within the group must agree on the use of a hash-function (for example one of the functions specified in ISO/IEC 10118).

d) Every entity wishing to act as a claimant must be equipped with an asymmetric key pair, selected as described below.

e) Every entity wishing to act as a verifier must be equipped with a means to obtain trusted copies of the public verification keys for the entities whose identities it is to verify.

NOTE — The exact means by which entities are provided with trusted copies of public verification keys is beyond the scope of this standard. This may, for example, be achieved by the use of public key certificates or by some other environment-dependent means.

6.2 Key selection

Each entity X wishing to act as a claimant in this mechanism must be equipped with an asymmetric key pair (y_X, z_X), where z_X (the private key) shall be an integer chosen to satisfy $0 < z_X < q$. The corresponding public verification key y_X shall be set equal to $g^{z_X} \bmod p$.

NOTE — Guidance on the choice of parameters for this mechanism is given in Annex B.

6.3 Authentication exchange

This unilateral authentication mechanism involves the following exchanges of information between a claimant A and a verifier B, and enables B to check the identity of A.

The authentication mechanism is illustrated in figure 2. The bracketed numbers in the figure correspond to the steps of the exchange described in detail below.

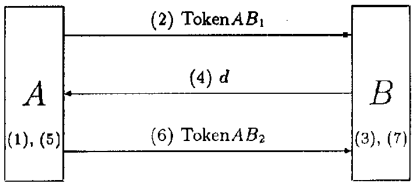


Figure 2 — Discrete logarithm based mechanism

The form of the first token (TokenAB_1), sent by the claimant to the verifier is either:

$$\text{Token}AB_1 = W$$

or

$$\text{Token}AB_1 = h(W||\text{Text})$$

where W is the witness, h is a hash-function, and Text is an optional text field. This text field is available for use in applications outside the scope of this part of ISO/IEC 9798 (it may be empty). See annex A of ISO/IEC 9798-1 for information on the use of text fields. If this Text field is non-empty then B must have the means to recover the value of Text; this may require A to send all or part of the Text field with TokenAB_1 (see also Note 1 below).

The form of the second token (TokenAB_2), sent by the claimant to the verifier is:

$$\text{Token}AB_2 = D$$

where D is the response.

(1) Entity A chooses a random number r, subject to the restriction that r shall be an integer satisfying $1 < r < q$. This integer is kept secret by A. A now computes the witness W as

$$W = g^r \bmod p.$$

(2) A sends TokenAB_1 to B. TokenAB_1 shall be equal to either W or $h(W||\text{Text})$.

(3) Having received TokenAB_1, B shall choose at random an integer d (the 'challenge'), where d shall satisfy $0 \leq d < q$.

(4) B sends the challenge d to A.

(5) On receipt of the challenge d, A shall compute the response D from the (secret) value r and A's private key z_A by:

$$D = r - dz_A \bmod q.$$

(6) A sends Token$AB_2 = D$ to B.

(7) On receipt of the response D, B shall perform the following computations.

(a) B checks that $0 < D < q$. If not then B shall reject A.

(b) B computes the value W' using the following formula:

$$W' = (y_A)^d g^D \bmod p.$$

(c) If W was sent in the first exchange of the procedure then B checks that the computed value W' is equal to the value of W sent in the first exchange of the procedure. Alternatively, if $h(W||\text{Text})$ was sent in the first exchange of the procedure, then B computes $h(W'||\text{Text})$ and then checks it is equal to the value of $h(W||\text{Text})$ sent in the first exchange of the procedure. If $h(W||\text{Text}) \neq h(W'||\text{Text})$ then the mechanism has failed and A shall be rejected. Otherwise B accepts A.

NOTE 1 — Other information may be sent with any of the exchanges of any of the iterations of the authentication procedure.

NOTE 2 — It is important that A chooses the random value r by a process which guarantees that selected values are independent within the lifetime of the accreditation information. If, for example, the same value r is used twice, then a third party may be able to deduce the private accreditation information of A, and hence be able to impersonate A successfully.

NOTE 3 — It is recommended that the key pair used in this mechanism be used only for the purposes of authentication, and should not be used for any other application (e.g. generation of digital signatures). If this recommendation is not followed then special care should be taken to prevent the verifier using the claimant as a 'signing oracle'; this could, for example, be achieved by requiring the challenge to be of a specially chosen form.

NOTE 4 — The use of $h(W||\text{Text})$ instead of W in the first exchange of the procedure can achieve efficiency gains by reducing the number of bits in TokenAB_1.

7 Certificate-based mechanism using an asymmetric encipherment system

In this clause an entity authentication mechanism is specified which uses an asymmetric encipherment system.

NOTE — This mechanism is derived from the Brandt-Damgard-Landrock-Pedersen scheme, [1,8].

7.1 Specific requirements

In order to use the mechanism within a group of entities, the following steps shall be taken.

a) Every entity wishing to act as a verifier must have the means to generate random numbers.

b) All entities within the group must agree on the use of two cryptographic functions: an asymmetric encipherment system, and a hash-function (for example one of the functions specified in ISO/IEC 10118).

c) Every entity wishing to act as a claimant must be equipped with an asymmetric key pair for use with the asymmetric encipherment system.

d) Every entity wishing to act as a verifier must be equipped with a means to obtain trusted copies of the public keys for the entities whose identities it is to verify.

NOTE — The exact means by which entities are provided with trusted copies of public keys is beyond the scope of this standard. This may, for example, be achieved by the use of public key certificates or by some other environment-dependent means.

7.2 Authentication exchange

This unilateral authentication mechanism involves the following exchanges of information between a claimant A and a verifier B, and enables B to check the identity of A.

The authentication mechanism is illustrated in figure 3. The bracketed numbers in the figure correspond to the steps of the exchange described in detail below.

The form of the token (TokenBA) sent by the verifier to the claimant is:

$$\text{Token}BA = d$$

where d is the challenge. The form of the token (TokenAB) sent by the claimant to the verifier is:

$$\text{Token}AB = D$$

where D is the response.

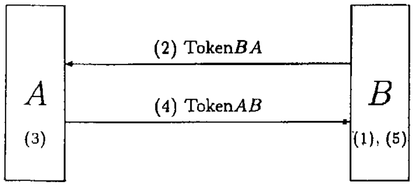


Figure 3 — Trusted public transformation based mechanism

(1) Entity B chooses a random number r. This number is kept secret by B. B next computes $h(r)$. The random number r shall be chosen in such a way that $r||h(r)$ lies within the domain of P_A, the public encipherment transformation of A. B now computes the challenge d as

$$d = P_A(r||h(r)).$$

(2) B sends Token$BA = d$ to A.

(3) Having received TokenBA, A performs the following computational steps.

(a) A recovers the value r by calculating

$$r||h(r) = S_A(d),$$

where S_A is the private decipherment transformation of A.

(b) A recomputes $h(r)$ from the recovered value of r, and if this value is not equal to the value received from TokenBA then A aborts the mechanism. If the computed value of $h(r)$ is the same as the value recovered from TokenBA then A sets $D = r$.

(4) A sends Token$AB = D$ to B.

(5) On receipt of TokenAB, B compares D with r. If $r \neq D$ then the mechanism has failed and A is rejected. If $r = D$ then B accepts A.

NOTE 1 — Other information may be sent with either of the exchanges of this mechanism.

NOTE 2 — It is important that B chooses the random number r by a process which guarantees that the probability of the same number r being chosen twice within the lifetime of the asymmetric key pair of A is vanishingly small. If the same number r is used twice, then a third party who intercepts the response D on the first occasion that it is sent, will be able to impersonate A to B by replaying D as a response to B after B has sent the number r the second time. However, re-use of a previously valid value of r will only invalidate one particular instance of use of the mechanism.

NOTE 3 — It is recommended that the key pair used in this mechanism be used only for the purposes of authentication, and should not be used for any other application (e.g. encryption of messages). If this recommendation is not followed then special care should be taken to prevent the verifier using the claimant as a 'decrypting oracle'; this could, for example, be achieved by requiring the hash-value $h(r)$ to be of a special form.

Annex A
(informative)
Principles of zero knowledge mechanisms

A.1 Introduction

In the context of the use of asymmetric cryptographic techniques, a potential weakness of an authentication exchange is that the verifier may abuse the mechanism to compromise the claimant's private key. When asymmetric cryptography is being used, the claimant uses the private key of his asymmetric key pair to compute the response to a verifier's challenge. The verifier may then, by choosing the challenge wisely, gain information about the private key of the claimant that could not have been obtained just from knowledge of the public key of the claimant.

This type of abuse of an exchange of cryptographic messages is known as using the claimant as an 'oracle', in that the claimant provides information about his private key at the behest of the verifier. The idea behind a zero-knowledge authentication mechanism is simply to remove this particular potential threat by careful design of the messages. This is done by ensuring that the verifier cannot use the claimant as an oracle.

A.2 The need for zero-knowledge mechanisms

In applications involving modern computer networks, the need for security services such as user authentication, non-repudiation, etc. is widely recognized and steadily growing. In order to be able to use such services, it is necessary for a user to have access to private information, specific to that user. Examples are passwords, private keys to a digital signature system, etc.

It is of course mandatory for the security of the system that the private information stays private, i.e. does not leak to other potentially hostile parties. On the other hand, the private information must be used as input to the soft- or hardware modules that compute and send messages on behalf of the user. If the information is not properly used, the secrecy of the private information may be damaged, or even destroyed completely. An obvious example is when users identify themselves to a host by sending a password in cleartext. This reveals totally the private information with the immediate result that anyone eavesdropping on the line can impersonate all users whose passwords have been intercepted.

This is an example where too much information is being communicated. To illustrate this, note that from the point of view of the host, there are only two possibilities: either the user possesses the correct password or he does not. In information theoretic terms, this means that only 1 bit of information really needs to be communicated. By sending the entire password, we therefore communicate much more than is needed, and this is the theoretical background for the practical problem of eavesdropping.

It is natural to ask: can one design protocols for use of private information which communicate exactly the information they are meant to communicate, and nothing more? Informally, this is precisely the property that a zero-knowledge mechanism has. Consider for example a situation where user A is assigned a key pair for a asymmetric cryptographic system (P_A, S_A), such that P_A is public while S_A is private to A. Then using a zero-knowledge mechanism, A can convince B that A possesses the private key corresponding to P_A, without revealing anything other than this fact. Since A is characterized as the only user with access to S_A, this protocol can be used for authentication. In this case, the zero-knowledge property guarantees that B will learn nothing that could help him to later falsely impersonate A.

The zero-knowledge property is achieved by designing a dialogue which can be simulated by the verifier alone. This intuitively proves that the verifier will learn nothing from the claimant in terms of properties of the claimant's private key, which the verifier could not have obtained himself from the corresponding public key. It also means that an observer to the exchange of messages making up the mechanism will be unable to decide if the claimant really was involved, or the exchange was simulated by the verifier.

Zero-knowledge mechanisms by nature require the use of asymmetric cryptographic techniques. Given the strict definition of a zero-knowledge mechanism, it is actually not possible to implement one. In fact, a much better description of the mechanisms in this part of ISO/IEC 9798 would be: 'Secrecy-protecting mechanisms'. However, the concept of zero-knowledge mechanism is part of a well-known and established theory in crypto-graphy, for which reason the terminology is used here.

A.3 The definition

Going a little closer to a formal definition, a zero-knowledge mechanism takes place between two parties, a claimant A and a verifier B. The claimant tries to convince the verifier that a certain statement is true. For example, this statement could be "I know the private key corresponding to P_A". To convince B, the claimant and verifier exchange messages for a while, after which B decides to accept or reject the claimant's proof.

Three essential properties are needed for such a mechanism:

— **Completeness.** If A's statement is true, then B should accept it with overwhelming probability.

— **Soundness.** If A's statement is false, then no matter how A behaves, B should reject it with overwhelming probability.

— **Zero-knowledge.** No matter how B behaves, he receives only the information that A's statement is true. A little more precisely: whatever B receives when talking to a truthful claimant, B could just as easily compute himself without talking to A at all. What this means is that B can simulate the conversation by himself, producing a conversation that looks exactly as if it had been generated by talking to A.

A.4 An example

Consider the following example, which is a simplified version of the Fiat-Shamir mechanism, [3]. Here, we are given a modulus n and a number modulo n, called y. In this case, A's statement is "I know a square root modulo n of y". Note that x is a square root modulo n of y, if and only if $x^2 \bmod n = y$.

The conversation between A and B goes as follows:

```
repeat $t$ times:

1. $A$ chooses $r$ at random (where
$2 \leq r \leq n-1$), squares it modulo $n$ and sends
the square to $B$.

2. $B$ chooses the bit $b$ equal to either 0 or
1 at random and sends it to $A$.

3. If $b$ equals zero then $A$ sends

                    $z = r$

to $B$. Otherwise $A$ sends

                    $z = rx \bmod n$,

where $x$ is the square root of $y$ modulo $n$,
which is known by $A$.

4. $B$ first checks that $z \neq 0$; if $z = 0$ then
$B$ rejects $A$ and aborts the procedure. If $b$
equals zero $B$ then checks that

                    $z^2 \equiv r^2 \pmod{n}$.

Correspondingly, if $b$ is equal to one then $B$
checks that

                    $z^2 \equiv r^2 y \pmod{n}$.

If the check is correct then continue, else
$B$ rejects and aborts the procedure.
```

It is not too difficult to see that if both A and B follow this procedure, then B will never reject A; squaring z means squaring either r or rx, which will give the result $r^2 \bmod n$ or $(rx)^2 = r^2x^2 = r^2y \bmod n$.

On the other hand, if in any of the t iterations, A is able to give a correct answer to both $b = 0$ and $b = 1$, this means that A can provide both z_0 and z_1, such that

$$z_0^2 = r^2 \bmod n$$

and

$$z_1^2 = r^2 y \bmod n.$$

By inserting the first equation in the second, it is straightforward to see that the number $z_1/z_0 \bmod n$ is a square root of y ($z_0 \neq 0$ and z_0 must be relatively prime to n with overwhelming probability). If A can compute z_1 and z_0 with this property, then he can compute z_1/z_0, and so his statement that he knows a square root of y is true. But conversely, if A is cheating and does not know a root of y, he must be unable to answer at least one value of b correctly in each of the t iterations. Therefore the probability that a cheating claimant convinces the verifier is at most 2^{-t}. For example, by doing 20 iterations, we reduce this chance to about 1 in a million. Thus the soundness property is also satisfied. As for zero-knowledge, note that all the verifier is left with after the conversation is over is two numbers z and r^2, such that either

$$z^2 \equiv r^2 \pmod{n}$$

or

$$z^2 \equiv r^2 y \pmod{n}.$$

But this is indeed something that the verifier could make himself without talking to A. To do this B just chooses a random z and either defines

$$r^2 = z^2 \bmod n$$

or defines

$$r^2 = z^2/y \bmod n.$$

The fact that r^2 and z are, in this case, computed in a way different from the way the claimant would compute them is insignificant; they are distributed in exactly the same way, i.e. it is impossible to tell the difference. Therefore, B learns nothing he could not compute himself, except for the fact that A knows a root of y.

Let us anticipate here an often asked question. If the verifier can make good looking conversations himself, without knowing a root of y, why should he be convinced when the claimant generates a similar conversation? The answer is that when B simulates the protocol, he is free to generate the number in a 'backwards direction', i.e. to first choose z and then find an r^2 that fits. In a real protocol execution, A does not have this opportunity. The verifier expects to see r^2 before b is chosen, and then the claimant must find a correct z.

Although we have glossed over a couple of technical difficulties here, these are the essentials of the argument why a mechanism has the zero-knowledge property.

A.5 Basic design principles

The example from the previous section covers one of two basic design ideas that underlie almost all known zero-knowledge mechanisms, namely:

> The claimant sends a 'witness' to the verifier. Then B asks A one out of some set of questions. If A is cheating, he cannot answer all possible questions, so we have some chance of catching him. On the other hand A never answers more than one question, and this one answer alone reveals nothing to the verifier.

This design idea forms the basis of the mechanisms specified in clauses 5 and 6.

The other design idea, and one which forms the basis of the mechanism specified in clause 7, is based on the following:

> The verifier asks the claimant a question, for which the verifier already knows the answer. The protocol must ensure that this really is the case. If A is honest, he can easily compute the right answer, but if he is cheating, he can do no better than guess at random, and will be incorrect most of the time.
>
> On the other hand, when B receives the answer, he already knows what A will say, and therefore the mechanism has the zero-knowledge property.

One easy example of this is when A must prove possession of a private key in a public key system. The verifier can encipher a random message under A's public key, and ask A to return the deciphered message. Only the user knowing the correct private key can do this. To get the zero-knowledge property, we must ensure that B really knows the message in advance. This standard contains an example of one way to do this, namely B can be asked to reveal some information (the *witness*) related to the message.

A formal basis for a rigorous understanding of zero-knowledge protocols is given in [2] and [4].

Annex B
(informative)
Guidance on parameter choice

This annex provides guidance on parameter choice for two of the mechanisms defined in this part of ISO/IEC 9798.

B.1 Parameter choice for the identity-based mechanism

Guidance is provided on the choice of the parameters m, n, p, q, v and t. Note 2 in clause 5.2 of this part of ISO/IEC 9798 is also relevant to the choice of these parameters.

a) The modulus n. As stated in clause 5.2, the prime numbers p and q shall be chosen in such a way that knowledge of their product n shall not feasibly enable any entity to deduce them, where feasibility is defined by the context of use of the authentication mechanism.

b) The public accreditation verification exponent v. Certain small prime values of v, e.g. 2, 3 or $2^{16}+1$ (in the latter case typically combined with $t=1$ or 2) have some practical advantages in reducing the computational complexity of calculating the witness W; in general the choice of a relatively small value for v will reduce the complexity of calculations for the claimant.

c) The multiplicity parameters m, t. The value v^{-mt} is equal to the probability that a false claimant can succeed in a masquerade attack by 'guessing' the value(s) of the challenges $d_1, d_2, \ldots, d_m$ in advance in each of the iterations of the protocol. Thus m and t should be chosen so that v^{-mt} is less than a probability threshold value which will depend on the sensitivity of the application. For most applications a value between 2^{-16} and 2^{-40} will be appropriate, where the exact value chosen will depend on the risk assessment.

The form of the identification data to be used in conjunction with this mechanism needs to be chosen with care, especially if identification data may need to be revoked or expired should the private accreditation information corresponding to the identification data become compromised. More specifically, expiry of an entity's identification data can be enforced by the inclusion of an expiry date in the identification data. This expiry information can be made available to the verifier by including it in the first exchange of the first of the t iterations of the authentication procedure.

In a similar way revocation of an entity's identification data can be enforced by the inclusion of a serial number in the identification data. The verifier can then check this serial number against a 'blacklist' of revoked identification data.

B.2 Parameter choice for the certificate-based mechanism using discrete logarithms

Guidance is provided on the choice of the parameters d, g, p and q.

a) The prime numbers p, q and the base g. As stated in clause 6.1, the values p and g shall be chosen so that, given an arbitrary integer i $(1 < i < q)$, finding an integer j (if one exists) such that $g^j \bmod p = i$ shall be computationally infeasible. Such an integer j is commonly known as the discrete logarithm of i to the base g modulo p.

Computational feasibility is defined by the context of use of the authentication mechanism. The bit lengths of the primes p and q provide lower bounds on the complexity of computing discrete logarithms, and thus the lengths of p and q must be chosen with care.

The prime p can be chosen so that a copy of the binary representation of q is embedded within the binary representation of p. Such an approach for choosing p and q may be useful in situations where storage space and/or communications bandwidth is at a premium. Annex C.2.1.1 provides an example of such a pair p, q.

If there is an odd factor smaller than q dividing $p-1$, then the user key may be compromised by an attack of the type described in [7]. To prevent such an attack, p and q should be chosen so that $(p-1)/2q$ has no prime factors smaller than q. Ideally, $(p-1)/2q$ should be prime.

b) The challenge d. Suppose d is chosen at random from the range $0 \leq d \leq 2^D - 1$ for some positive integer D. The value 2^{-D} is equal to the probability that a false claimant can succeed in a masquerade attack by 'guessing' the value of the challenge d. Thus D (the bit length of d) should be chosen so that 2^{-D} is less than a probability threshold value which will depend on the sensitivity of the application. For most applications a value between 2^{-16} and 2^{-40} will be appropriate, i.e. a value for D between 16 and 40, where the exact value chosen will depend on the risk assessment.

Annex C
(informative)
Examples

This annex gives examples for the computation of the entity authentication mechanisms specified in this part of ISO/IEC 9798. Throughout this annex integers are given in hexadecimal representation.

The examples given here are intended for illustration and as an aid to validating practical implementations only, and should not be used in practice.

C.1 Mechanism based on identities

C.1.1 Example with public exponent 2

C.1.1.1 Parameter selection

In this example the public verification exponent v is 2, which is even. Therefore the secret prime factors p and q must satisfy:

$$\gcd(\frac{p-1}{2}, v) = \gcd(\frac{q-1}{2}, v) = 1,$$

and

$$p - q \text{ is not a multiple of 8.}$$

p = f859 cdc6 f78f d206 a8d2 e78c bfc8 2735 5798 5d16 cbf9 431f abfc c16f 9ca9 3a5e f099 d3e8 3fe0 c67e 31f5 77dd ccf1 8287.

q = fef3 6abf 2aaf afa7 1c0b ca24 efe2 fb28 3366 1fb9 266f 9046 3c78 aa54 4a7c e2d8 9e56 071e 42db 00b3 c87e dc89 563a 02fb.

The public modulus n is 768 bits long.

n = f755 3ef8 611b c569 0a2e 4d13 801a 94be 4dc8 fe2d da6c 6e11 586e 1941 81fb 96bf dc09 4d04 edbe ed1d 22ce 1fae 689b a233 3298 7fd7 9ef8 715f 1f5a 5eb4 b41f 45ea fcc5 4f32 5f21 5135 2930 8ff9 d8cd 5738 3801 fce9 7b51 f50f 8192 b0e1 c066 085d.

$k_s = 767$.

The accreditation authority's private accreditation exponent u is the least positive integer satisfying: $uv + 1$ is a multiple of $\frac{\mathrm{lcm}(p-1,q-1)}{2}$.

u = 1eea a7df 0c23 78ad 2145 c9a2 7003 5297 c9b9 1fc5 bb4d 8dc2 2b0d c328 303f 72d7 fb81 29a0 9db7 dda3 a459 c3f5 cd13 7446 2769 68ea 2f97 1df6 2b4f 75a0 608e 8471 ae38 da4c 4d97 0fb9 e817 6486 be34 e740 1522 443c 5f12 c5bb b0e3 cb8f 53a7 505b.

$m = 8$; $l = 3$.

C.1.1.2 Identity selection

The identification data consists of a sequence of $m = 8$ parts. These identity parts are constructed using the string 'Alex Ample' postfixed with a 16-bit field number.

I_{A1} = 416c 6578 2041 6d70 6c65 0001
I_{A2} = 416c 6578 2041 6d70 6c65 0002
I_{A3} = 416c 6578 2041 6d70 6c65 0003
I_{A4} = 416c 6578 2041 6d70 6c65 0004
I_{A5} = 416c 6578 2041 6d70 6c65 0005
I_{A6} = 416c 6578 2041 6d70 6c65 0006
I_{A7} = 416c 6578 2041 6d70 6c65 0007
I_{A8} = 416c 6578 2041 6d70 6c65 0008

C.1.1.3 Accreditation generation

J_{A1} = 5341 276c 2465 f078 5e20 9341 2a6d fe70 276c 2465 ee00 e301 9341 276c 2465 f078 5e20 9341 2a6d fe70 276c 2465 ee00 e301 9341 276c 2465 f078 5e20 9341 2a6d fe70 276c 2465 ee00 e301 9141 276c 2465 f078 5e20 9341 2a6d fe70 276c 2465 ee00 e316.

C_{A1} = 79b7 7f76 b264 a2e0 bc4c e8f9 f29a 2175 99b4 2567 6dda 9360 228b ede5 748a d735 b2e9 bcf8 de99 6c8a 87db f920 26f4 b81e f97f 2b18 e50c 526b 2a40 f619 7d72 d7da 7d2e a641 2c2a fd97 df62 dfc4 56eb b043 8a99 1880 8749 387a 4a52 4a78 5049 4be6.

J_{A2} = 29a0 93b6 1232 f83c 2f10 49a0 9536 ff38 13b6 1232 f700 7281 49a0 93b6 1232 f83c 2f10 49a0 9536 ff38 13b6 1232 f700 7281 49a0 93b6 1232 f83c 2f10 49a0 9536 ff38 13b6 1232 f700 7281 48a0 93b6 1232 f83c 2f10 49a0 9536 ff38 13b6 1232 f700 7293.

C_{A2} = 41fb 8c2e c141 60fc 896b 1f36 d68a 4f8e 7a31 1226 31e2 28ea 568e c98e b09a 0e88 3500 21c1 8ac6 f81a 9f29 e8d2 25b0 8795 40b8 1791 e0ff 0cab 4aca 6e7c e17d c59c bc7e c931 9d92 beb5 8433 111e 14fd f601 6494 536f 2bc9 c692 a1f0 1da5 bd5d 8b90.

J_{A3} = 29a0 93b6 1232 f83c 2f10 49a0 9536 ff38 13b6 1232 f700 7401 c9a0 93b6 1232 f83c 2f10 49a0 9536 ff38 13b6 1232 f700 7401 c9a0 93b6 1232 f83c 2f10 49a0 9536 ff38 13b6 1232 f700 7401 c8a0 93b6 1232 f83c 2f10 49a0 9536 ff38 13b6 1232 f700 741b.

C_{A3} = 03c1 c485 28ac 5b9b 639a 0123 c093 6f2e d642 89e2 799a a434 2377 92d3 3ef2 d055 2cd8 3cfc 68ea 6a70 e310 1e72 5724 9c92 48e9 fd19 7ff1 d126 4c62 2ba8 8cac f99f daed 0adc e206 7e29 9dd9 0a15 3868 5d3b 396a af56 0332 fc84 46d0 2ab5 69fa 6cc6.

J_{A4} = 5341 276c 2465 f078 5e20 9341 2a6d fe70 276c
2465 ee00 e904 9341 276c 2465 f078 5e20 9341 2a6d
fe70 276c 2465 ee00 e904 9341 276c 2465 f078 5e20
9341 2a6d fe70 276c 2465 ee00 e904 9141 276c 2465
f078 5e20 9341 2a6d fe70 276c 2465 ee00 e946.

C_{A4} = 0e78 f7fe d61e 0934 ce1d 5c30 e3d8 7e50 def0
f339 06ff cadb ac33 fced 95c4 8579 d651 33fe 1bd6
963a 8a1e 56c5 d318 a94c fdab 5c27 9a61 25c5 07ed
d1da 4aec a673 47cc 78f6 6a2b a671 e432 5d94 3b18
ad1e a2f2 f51e 2301 5070 ede3 fd92 5291 1ea2.

J_{A5} = 29a0 93b6 1232 f83c 2f10 49a0 9536 ff38 13b6
1232 f700 7202 c9a0 93b6 1232 f83c 2f10 49a0 9536
ff38 13b6 1232 f700 7202 c9a0 93b6 1232 f83c 2f10
49a0 9536 ff38 13b6 1232 f700 7202 c8a0 93b6 1232
f83c 2f10 49a0 9536 ff38 13b6 1232 f700 722b.

C_{A5} = 2be9 2edd 3b6c 4977 ffe7 3b6f d0c9 1835 1b04
2b0a 33b9 7fb1 d407 724c 5035 a335 109e 791f a4b7
03f2 d8be 9a8e 031e bad6 7175 90c7 ad03 9250 9f4b
177b 40f6 0653 9eb7 6d1d 49e8 949e bc12 989f ad28
675e 8dd2 eb59 e5fc 4703 2ef1 b9a1 da84 b8d1.

J_{A6} = 5341 276c 2465 f078 5e20 9341 2a6d fe70 276c
2465 ee00 e206 9341 276c 2465 f078 5e20 9341 2a6d
fe70 276c 2465 ee00 e206 9341 276c 2465 f078 5e20
9341 2a6d fe70 276c 2465 ee00 e206 9141 276c 2465
f078 5e20 9341 2a6d fe70 276c 2465 ee00 e266.

C_{A6} = 1ae7 264d 6b92 9c8d 3131 5411 e0b0 65c1 9ac2
c815 a6dc 92bd 26e8 2281 8ce8 d9b0 bde2 b895 a267
f6eb 226e 3989 fed6 fac0 1865 66f0 9bed 5992 b882
02c1 2df7 e903 3849 4881 8570 298d 8df1 27c4 4758
f769 ccf4 a6ce 2303 3fb0 b13c 17c9 8eb7 7db4.

J_{A7} = 5341 276c 2465 f078 5e20 9341 2a6d fe70 276c
2465 ee00 ef07 9341 276c 2465 f078 5e20 9341 2a6d
fe70 276c 2465 ee00 ef07 9341 276c 2465 f078 5e20
9341 2a6d fe70 276c 2465 ee00 ef07 9141 276c 2465
f078 5e20 9341 2a6d fe70 276c 2465 ee00 ef76.

C_{A7} = 496f db6e e535 0180 1c86 6610 8769 f225 4631
6b07 0267 d57d 7613 f42c 70e1 0d39 256f 5c60 3d22
7f28 5401 0d42 05d3 eab1 f795 b386 5595 4234 7f8a
3ce0 b483 8d7f 0cf2 dea6 f895 277a a2f5 1732 e854
8f44 d31a e502 ad03 7194 0d65 ab07 c55d c85f.

J_{A8} = 29a0 93b6 1232 f83c 2f10 49a0 9536 ff38 13b6
1232 f700 7004 49a0 93b6 1232 f83c 2f10 49a0 9536
ff38 13b6 1232 f700 7004 49a0 93b6 1232 f83c 2f10
49a0 9536 ff38 13b6 1232 f700 7004 48a0 93b6 1232
f83c 2f10 49a0 9536 ff38 13b6 1232 f700 7043.

C_{A8} = 4892 3caa be40 0643 ce8a 24ab 1e48 5876 ae94
9ae1 a465 ced2 a59e 63d2 fd37 044b 202e 1543 64db
38b5 d16a b675 2401 98be 23c1 ba7c ca8a 0058 4ae9
e637 f70a a640 c1a8 a1b3 2f5a 3a35 7e75 7df4 04e3
0ffb 8203 0b5c 986a 131b 1aa7 b37b 2c04 4dbe.

C.1.1.4 Authentication exchange

The authentication procedure is iterated $t = 3$ times.

Iteration 1:

Step (1):

r = f637 29e2 8723 3b12 d7c9 b048 8626 7680 3880
f8b8 0ba0 3497 60fe 2c2d ee4f a8ed 7860 8a3f 24f1
22f4 45d1 cb18 8ef2 82c1 a6ea 4453 c550 cfcf d16f
ebdb add9 51ed 750e d717 cd83 8cd3 1cbc ce82 c2e6
afe4 8507 e66b 5417 33eb d4e1 8c94 e180 e1c6.

W = 573c 7004 78cd feac 4025 4777 20fa 7e68 8010
deb9 0a10 676e e59b 9074 40be e961 86af f988 6449
1a34 aa7e b741 1af9 3e12 fd4b d9ff fc0b dfc9 5c1a
3780 8b77 aa8f 3170 e240 c6ae 9d03 c7d9 9acc e21b
f125 a4f7 9f16 f26d e6bf dcb2 d6ae 6187 d536.

Step (3):

$d_1, d_2, \ldots, d_8 =$ 0, 0, 1, 0, 1, 1, 0, 1.

Step (5):

D = 415c d169 1334 412a be2d 6bdd d373 305f 0eed
f1d2 f943 68e6 62cb da0e 9e46 8840 af85 9372 8fb5
6354 3bb5 7061 ff42 210d 6fbf 8232 3ef6 82a3 1956
2d57 3e06 0a6c 5c63 9762 a18a f0ca 12de e2bf f91d
c376 844a 7f14 6113 c6a3 269c 8211 2d62 cbc5.

Step (7c):

W' = 573c 7004 78cd feac 4025 4777 20fa 7e68 8010
deb9 0a10 676e e59b 9074 40be e961 86af f988 6449
1a34 aa7e b741 1af9 3e12 fd4b d9ff fc0b dfc9 5c1a
3780 8b77 aa8f 3170 e240 c6ae 9d03 c7d9 9acc e21b
f125 a4f7 9f16 f26d e6bf dcb2 d6ae 6187 d536.

Iteration 2:

Step (1):

r = 6d5f 2b2f 5027 39a9 177d 30f4 8d5e 1b6d 40d4
eea9 35d8 3bb4 0288 b447 6cdf 3f5c f0f9 b714 08dc
eaae ff5a b380 c96b acb0 973b 78ab 08f6 d085 795d
92e3 630b ffa8 59ae 1eb5 2b52 0c5d 6030 fe80 a4e1
1a2f ed3d 6801 5311 a0ab 5018 8a73 f1b6 9460.

W = 44ce 41f4 9c42 ec82 f5ac 5a42 03e6 6cc5 bcb6
f343 f0db 0c07 5318 fc26 328f 1f07 35df 653b c8bc
9bf9 a6af fafe 98a5 14d6 4952 1f5b c1a9 de55 721e
8950 399d 7c3b cb2d ba2d ef50 5cce a17e e8ec 314a
6621 ccd4 5755 5136 b4f6 fdb6 b6de ce3d 94c9.

Step (3):

$d_1, d_2, \ldots, d_8 =$ 0, 1, 1, 0, 0, 0, 1, 0.

Step (5):

D = 0c84 7739 615a 2c11 a240 6314 bb0c 1bce 155f
b99e 7c92 8c3d 15a8 ee81 ea67 1f6d c248 d1c8 9c06
a80f b4e2 a2cb d5e3 54ca b5ba 98f6 f2ac e1f6 c160
dc82 8f8e db4f 2131 a11c 86a0 86ba 9f74 e838 b653
cd25 02cc 1877 1ed7 113c 1cb3 bf19 6cac 738f.

Step (7c):

W' = 44ce 41f4 9c42 ec82 f5ac 5a42 03e6 6cc5 bcb6
f343 f0db 0c07 5318 fc26 328f 1f07 35df 653b c8bc
9bf9 a6af fafe 98a5 14d6 4952 1f5b c1a9 de55 721e
8950 399d 7c3b cb2d ba2d ef50 5cce a17e e8ec 314a
6621 ccd4 5755 5136 b4f6 fdb6 b6de ce3d 94c9.

Iteration 3:

Step (1):

r = c50a 4b30 b2ad 7b7a 26ac 6ca5 0b2e 2d2c 0d40
1fb8 4e6d 6d12 3fce c8f2 9f55 26cf eced cbf0 184c
f826 5db5 db87 a82e 9397 9fd5 9152 b65a fdbd f5a2
c017 9781 33ab 12ec f85f 5db8 9fdb 6aa5 43b5 87b2
88f0 2963 4604 9703 5838 7cb3 28bd a1a9 b699.

W = 0268 2fb9 c79b 2c9f bdc3 2804 6dc5 9a30 d3c7
0e02 01db e43e 2c09 8fde f967 037f 20be 354e c92d
208e ecfd a688 7126 58cf 28fd c27c c97b 8520 a408
1570 0539 de84 632b 0ba2 b899 95c9 199e 9d61 a0cb
c036 2ed1 0a8e d566 4935 98cb 7f32 038d 525d.

Step (3):

$d_1, d_2, ..., d_8$ = 1, 1, 0, 0, 0, 0, 0, 1.

Step (5):

D = 3c61 982e fa0e 5c75 dada 504e d5e2 b056 e3cf
80bb fad1 2925 05bd 426c 952e bace ffd3 cdb3 cb5d
2233 7128 9507 81a0 464a f7cf db3e dbaa f76f 2d1a
d3c8 7ce2 5289 fe4d 87eb 9583 20ba 749a 369a da50
0227 bd8a 8439 8e8c 5a4e 82eb 90a1 0294 2448.

Step (7c):

W' = 0268 2fb9 c79b 2c9f bdc3 2804 6dc5 9a30 d3c7
0e02 01db e43e 2c09 8fde f967 037f 20be 354e c92d
208e ecfd a688 7126 58ef 28fd e27c c97b 8520 a408
1570 0539 de84 632b 0ba2 b899 95c9 199e 9d61 a0cb
c036 2ed1 0a8e d566 4935 98cb 7f32 038d 525d.

C.1.2 Example with public exponent 3

C.1.2.1 Parameter selection

In this example the public verification exponent v is 3, which is odd. Therefore the secret prime factors p and q must satisfy:

$$\gcd(p-1, v) = \gcd(q-1, v) = 1.$$

p = a0ca e977 6bc5 5a7f f591 7bc8 8164 16f9 503c
16e9 0a0c 4da3 b1d3 d97a 1220 605e 071f 1c6f 9305
def5 4832 0ea3 5e76 4d45 698e 9196 09a4 35f1 fde4
0d7c 3146 8eb3.

q = e349 3f5b 7808 aac9 6083 b0b6 d97d 5a57 d300
43c8 6416 719e 2d95 7654 5f0a c7b1 4061 8232 728c
7777 0fbe aac2 f5f0 8238 5783 91bb ceb5 be1e cd31
b043 be4f 75df.

The public modulus n is 1024 bits long.

n = 8ec1 eeac da97 aa8b a6e2 fb76 4423 dcc7 d723
2848 5219 c685 bcef f9a8 f970 a9b2 ed4d 7dd8 64dd
162d f77a a9b8 549e 7029 d409 9494 61af 3590 e5ca
6cf4 1f5b 073d b399 f566 0068 4ff9 60f8 8336 85a6
d337 84c3 cade c2e9 32fe a1fe 9b05 85b2 8a8a 4b02
4bdb 7d46 9b62 2657 b19a ade2 768d 3608 f0be 09bb
9d59 c88c 7d3c 0eeb 1ced.

$k_s = 1023$.

The accreditation authority's private accreditation exponent u is the least positive integer satisfying: $uv + 1$ is a multiple of $\mathrm{lcm}(p-1, q-1)$.

u = 2f95 fa39 9e32 8e2e 8cf6 53d2 16b6 9eed 47b6
62c2 c608 9781 e9a5 5338 5325 8de6 4f19 d49d 76f4
5cb9 fd28 e33d 718a 2563 46ad dc31 75e5 11da f743
79a6 b51e 57be ba81 eedb b433 6e3a ae4b c792 6397
20a2 2082 7ab9 c6ec d13e eb87 1912 5c2d 20d3 abd5
e468 7d3c 16fc 9a22 52bc 1dd3 e25a 7c52 4479 65cb
386d a9d2 3fd4 0a71 b2c9.

$m = 5$. $t = 5$.

C.1.2.2 Identity selection

The identification data consists of a sequence of $m = 5$ parts. These identity parts are constructed using the string 'Alex Ample' postfixed with a 16-bit field number.

I_{A1} = 416c 6578 2041 6d70 6c65 0001
I_{A2} = 416c 6578 2041 6d70 6c65 0002
I_{A3} = 416c 6578 2041 6d70 6c65 0003
I_{A4} = 416c 6578 2041 6d70 6c65 0004
I_{A5} = 416c 6578 2041 6d70 6c65 0005

C.1.2.3 Accreditation generation

J_{A1} = 676c 2465 ee00 e301 9341 276c 2465 f078 5e20
9341 2a6d fe70 276c 2465 ee00 e301 9341 276c 2465
f078 5e20 9341 2a6d fe70 276c 2465 ee00 e301 9341
276c 2465 f078 5e20 9341 2a6d fe70 276c 2465 ee00
e301 9341 276c 2465 f078 5e20 9341 2a6d fe70 276c
2465 ee00 e301 9141 276c 2465 f078 5e20 9341 2a6d
fe70 276c 2465 ee00 e316.

C_{A1} = 2f98 686f a57f 0799 f0a6 42dc 20ae 91f4 f875
a346 a6b8 e951 042e 77c6 1ad9 0a60 915d 8ea6 9dbf
bec2 589f 331f 26a7 0859 9ca8 27b5 5a5c b78b ee4e
07b4 9c86 dd7e afea 5a4e 9b9d 068b 173d a27e ebc0
78b1 8305 e930 48db b81e 49cd 83f0 e101 260a 76bc
10d8 8679 5b4c b096 7943 5195 ea43 b98b 35a4 c3b1
eb02 8e7c 0f54 0949 67f8.

J_{A2} = 676c 2465 ee00 e502 9341 276c 2465 f078 5e20
9341 2a6d fe70 276c 2465 ee00 e502 9341 276c 2465

f078 5e20 9341 2a6d fe70 276c 2465 ee00 e502 9341
276c 2465 f078 5e20 9341 2a6d fe70 276c 2465 ee00
e502 9341 276c 2465 f078 5e20 9341 2a6d fe70 276c
2465 ee00 e502 9141 276c 2465 f078 5e20 9341 2a6d
fe70 276c 2465 ee00 e526.

C_{A2} = 31ca f31b 374b a31c ba12 b38a 23e8 46c7 dac1
7ead 4647 34e9 8adb 781b 4c56 2463 ced6 9ee3 6eae
0992 c2af 5027 5874 7b15 4f2d 723d a590 593a ec39
5fbd de29 7bc5 0fab 1af9 7143 a0d1 b25a b1bc 6c7f
544f 72a9 35ec 265d a54d d52d c5b6 cde9 58ef 593b
2dfa 5ba6 0c05 8f11 6c9f 488e d9fb 8680 112c ba35
aec8 7441 7aa5 8f4b 57f5.

J_{A3} = 676c 2465 ee00 e803 9341 276c 2465 f078 5e20
9341 2a6d fe70 276c 2465 ee00 e803 9341 276c 2465
f078 5e20 9341 2a6d fe70 276c 2465 ee00 e803 9341
276c 2465 f078 5e20 9341 2a6d fe70 276c 2465 ee00
e803 9341 276c 2465 f078 5e20 9341 2a6d fe70 276c
2465 ee00 e803 9141 276c 2465 f078 5e20 9341 2a6d
fe70 276c 2465 ee00 c836.

C_{A3} = 2dac 4f99 c5c7 6a01 56bf 01f1 d135 2b07 3742
cc23 9e43 eaed d6d3 0e9f 8c17 750d 0024 5099 8caa
7c76 526c adc6 cd78 74d9 90b3 bcbb abc0 603f 0431
ae82 81f0 2d92 4c8b 3add 7eb0 2c37 bca5 2ea5 c740
6752 0bdc 0644 a64e ae8e 6690 4ac0 31af cc8d 1c8b
1a4f 8c04 de6a bb29 3d98 7449 0a87 56e6 c54d 0259
07a3 136c a560 3c42 d0a1.

J_{A4} = 676c 2465 ee00 e904 9341 276c 2465 f078 5e20
9341 2a6d fe70 276c 2465 ee00 e904 9341 276c 2465
f078 5e20 9341 2a6d fe70 276c 2465 ee00 e904 9341
276c 2465 f078 5e20 9341 2a6d fe70 276c 2465 ee00
e904 9341 276c 2465 f078 5e20 9341 2a6d fe70 276c
2465 ee00 e904 9141 276c 2465 f078 5e20 9341 2a6d
fe70 276c 2465 ee00 e946.

C_{A4} = 10d9 1f22 933c 27c2 589b b1d0 0a27 767c 1465
b9de 1074 aaf5 e845 128c d422 8cb1 2688 7139 2526
7d7b 6e07 cf01 975e aeac 9b50 9e8b 2432 06de b57c
0676 5069 5ddb 2a53 419d 7703 30ca f37a e3d7 148e
8dab b8c9 dd68 359a cb64 7d4c bbf1 156b 5aa8 49f0
7e12 3e0f d71c 853a d005 a36b 9bf9 ee65 3e12 cc18
4fa1 a3b8 9ee2 a121 353c.

J_{A5} = 676c 2465 ee00 e405 9341 276c 2465 f078 5e20
9341 2a6d fe70 276c 2465 ee00 e405 9341 276c 2465
f078 5e20 9341 2a6d fe70 276c 2465 ee00 e405 9341
276c 2465 f078 5e20 9341 2a6d fe70 276c 2465 ee00
e405 9341 276c 2465 f078 5e20 9341 2a6d fe70 276c
2465 ee00 e405 9141 276c 2465 f078 5e20 9341 2a6d
fe70 276c 2465 ee00 e456.

C_{A5} = 171d fcf1 dcda 63b1 a53c 1f8b a8a7 d46c 8ced
c942 956d 9fea 5469 61dc cc52 dcd8 4821 604e bde1
cd25 d23d 7815 0bdc 85b3 7aa0 b691 9609 6aac 6ca3
e843 5575 4eb1 2470 234d 05ea 8a46 45c2 fa69 eaac
e374 78d2 7394 12db 57c7 9018 6a85 8a00 8e56 732d
71f3 f5ea dc8e 0988 95cf 3a50 cfd8 e106 b640 2c9c
9c07 c630 6e15 ead4 e050.

C.1.2.4 Authentication exchange

Iteration 1:

Step (1):

r = 0fdf 125c 140e 2a4f 54d4 ef3b 41a4 e11e 7175
4f7b f003 1d01 8a51 8ac2 27be 49fa 6987 e987 ebb1
0ebb dbfd ee1a 9443 7313 fc53 44e0 5238 0a7f 155a
9ad0 70fd e4ef eb37 e6fb 1a82 d078 bc73 31a1 b95b
58e2 3665 ce63 1300 e862 2d52 5552 dd45 fdde e10e
f0e5 5d63 106c 0692 5dd8 4b1c ba98 fa0c 4e57 1a0b
135e c5d2 9659 47bf 7145.

W = 2935 3492 54b4 b32c fa87 b7af 0a17 12ef 568b
c5d9 593d f8a6 2972 b911 18c1 9d2e 5cee 57a5 1318
d878 e829 e9e7 0306 f482 e81f 57e4 e18d d71d 5312
a0a7 3539 971a e02f 46b4 1e8a 456e 9260 4090 8018
9c7a dfea d147 d75c 2aea 143e d666 c3b4 3993 616b
f040 c310 7baf 4584 c2e7 ec50 b8b2 040d c803 19c4
4faf 7b00 b3b0 67ab 8ee2.

Step (3):

$d_1, d_2, \ldots, d_5 = 2,\ 1,\ 2,\ 1,\ 2.$

Step (5):

D = 2381 3185 d61b 1684 1c72 8b6d eb9e 30a6 6b7f
c509 3c00 c5de 6194 9ba2 9721 a8df fe0d 04e5 f5c5
2e71 ac97 b511 a144 d4e9 7d5b 359d 1e92 ffb9 ca3a
2e61 42a8 a0a2 b3cd 22ee 1e28 5432 d645 21d4 73f6
d9b0 5765 22fb 3ea0 78ba 1ee4 f70c 8d56 d354 df85
a7e3 1257 f9c2 2865 d0e9 2f8a e587 61b0 4f04 4dd2
8b74 cf60 b332 d461 e5c7.

Step (7c):

W' = 2935 3492 54b4 b32c fa87 b7af 0a17 12ef 568b
c5d9 593d f8a6 2972 b911 18c1 9d2e 5cee 57a5 1318
d878 e829 e9e7 0306 f482 e81f 57e4 e18d d71d 5312
a0a7 3539 971a e02f 46b4 1e8a 456e 9260 4090 8018
9c7a dfea d147 d75c 2aea 143e d666 c3b4 3993 616b
f040 c310 7baf 4584 c2e7 ec50 b8b2 040d c803 19c4
4faf 7b00 b3b0 67ab 8ee2.

Iteration 2:

Step (1):

r = 583e 235e d777 a918 1d4a a2f9 da89 a905 3e65
a827 d573 c68e 73e7 ce5a 61b1 d135 1d6c 4236 df99
2c1a d174 588b 8e07 5f14 c954 44cf 3493 b44e 3971
dadc 38e6 3a86 a1c8 e4dc 222e 5290 86a3 3301 cd87
5be2 3c5b d963 df15 3f4b add7 4ea5 3eb5 f7a5 41d3
90a0 99b3 78ad 46ac 635a 3bdf 72eb 959d 4e1c ca8c
12aa 4a34 38ce a016 556f.

W = 2f69 40df a78e 740f bf64 9f12 f55d 5081 ab45
d794 b08b c3f9 c98e d1de f793 7fa5 9b20 860b 9474
bd0e 4874 93b4 ec52 6c31 7e2f c250 3a4a 4951 1b0a
9b12 8e53 80a8 b58d beca 35c2 d633 5b80 f184 89fb
eed9 b3da f95f 71b2 0eb1 f6e9 c4f6 2054 7eff 0ac5

97b5 7fc3 7d89 e746 91d1 8517 440a 1d37 63fd 377d
09c7 5369 88c5 9389 d3f3.

Step (3):

$d_1, d_2, ..., d_5 = 1, 1, 0, 0, 0.$

Step (5):

D = 10bf ace9 3bc3 80e1 f8a8 9229 f66f d7af 5819
d745 be0b 7980 8df0 0692 2e8f bdef 8650 d311 2269
eae1 7bc2 a641 509d 1238 148d d07c ca97 3d1a 67c5
e34c 50e2 9ab8 52eb 42e7 e527 6eb3 6cfb 18dc ec2f
6939 9461 7f05 6320 94b7 8c07 87cc db53 8f85 d8be
6754 e39b 9f2e 30cc 935f c2da 97cd 60c6 99ba bfac
07fe 02ea 406a 613e 34ea.

Step (7c):

W' = 2f69 40df a78e 740f bf64 9f12 f55d 5081 ab45
d794 b08b c3f9 c98e d1de f793 7fa5 9b20 860b 9474
bd0e 4874 93b4 ec52 6c31 7e2f c250 3a4a 4951 1b0a
9b12 8e53 80a8 b58d beca 35c2 d633 5b80 f184 89fb
eed9 b3da f95f 71b2 0eb1 f6e9 c4f6 2054 7eff 0ac5
97b5 7fc3 7d89 e746 91d1 8517 440a 1d37 63fd 377d
09c7 5369 88c5 9389 d3f3.

Iteration 3:

Step (1):

r = 170d 20a2 00f4 7124 fac0 695d 1612 07ce 848a
cba5 d1f5 adcb 0ab1 ae12 6377 4b5a 4ea1 48e2 434a
804b e374 6787 a775 29c9 59de c8c5 2952 cade 4d81
3061 6f6d f1ba b7b6 2b24 be92 5cfc 44e6 e2df 2b97
31c2 180f 3b32 c068 ee9f 0b70 88e0 e700 67d9 d799
0622 b329 bea3 c1f3 ff80 e614 3562 794a a065 28e8
61dd fc41 109c 6080 ded0.

W = 2c81 4f76 98b9 4169 b7c5 14a4 6f3c d9e9 5f7c
7aa1 9de9 9d59 fd42 7d8a 6f96 a45c 345c 823e e7ba
6dee 98a0 2c44 34b9 4249 32df 3ef8 4f79 4f8a 69d5
c970 a5f8 f8bc f1f7 4189 56a9 e9aa ae01 7928 2ccf
c1c8 5c75 1a7f a117 6c66 366d 8ee2 ef5d 9145 0aa1
18e4 1bc1 6601 373a 1340 72ba adb6 1565 e292 d826
0047 afb8 0b20 f227 2290.

Step (3):

$d_1, d_2, ..., d_5 = 0, 0, 1, 0, 2.$

Step (5):

D = 10fc 250c 11ad 61b8 19b1 eaa3 9376 4e22 cfce
7b98 af17 0d1e b74b a5c7 596b dafc f953 7fa6 c6d7
6fe9 61c1 c7bf 087b eb8d 25c8 74d9 ce81 959e f419
1912 927f da1c 04f7 92a6 dd1a 0ca3 7f86 2dc6 c4b9
331f 69a7 cd46 c7ad 7352 43d4 6223 ba0a c578 aaf4
1443 a413 67e7 5497 47e3 7603 ecad e131 f18a 771c
edd2 064c 5d56 11a9 7fa1.

Step (7c):

W' = 2c81 4f76 98b9 4169 b7c5 14a4 6f3c d9e9 5f7c
7aa1 9de9 9d59 fd42 7d8a 6f96 a45c 345c 823e e7ba
6dee 98a0 2c44 34b9 4249 32df 3ef8 4f79 4f8a 69d5
c970 a5f8 f8bc f1f7 4189 56a9 e9aa ae01 7928 2ccf
c1c8 5c75 1a7f a117 6c66 366d 8ee2 ef5d 9145 0aa1
18e4 1bc1 6601 373a 1340 72ba adb6 1565 e292 d826
0047 afb8 0b20 f227 2290.

Iteration 4:

Step (1):

r = 4224 ffa1 41bc 4bea 93d0 14ec acc1 fa5d 9616
f0fa c12a a029 3f84 a858 f916 13c3 ccef e0d1 16e5
30fc 4fda 72f5 15ce 5996 e211 fcc8 eee0 0719 84a6
b717 a7be cc05 afd1 8b8e 71ec 2d3f 285c 6d07 39c6
b4ef 3660 468d c13f 24c8 0ef8 c992 59f0 04c8 996e
9387 99a7 0769 03d7 fd23 9472 3396 6cc0 2ec3 fc30
33b9 4a8c d1fb 919f 610a.

W = 0525 c5ba f6f9 78b1 1fd6 6e86 0de3 ebd3 314e
efb0 9ca7 8193 3b2e cb5f 8046 1b46 a87a 727a a317
e163 9dc4 2b55 8202 65dd 0f2c ce4d 57fe 84dc 08f5
49ee 896a a897 c29a dabb e0c6 78fe 0be5 753d 0d97
0d99 f3d2 1eef b822 7715 39e7 402d 63da 03d4 b66f
3789 066e 4c36 d025 3466 1b6a e359 f290 bb21 c1fc
01fe 23fb 0135 77d8 0ea9.

Step (3):

$d_1, d_2, ..., d_5 = 0, 0, 0, 1, 2.$

Step (5):

D = 3559 cda5 4d03 1913 3dca c484 3a3f 9635 86e1
8455 3448 e759 1213 5269 9d8a 5a5d 4c4e 178e befd
7223 2808 356a 427a 0b1e 1681 3ba4 c564 27bf 0c03
1fb9 e35e ebcc 51c3 bfb2 346c 11f6 bc7c 3dfc d3f5
000d 2614 1ad5 7197 4362 f195 9750 a8ae 5750 f36d
fd40 b930 85ca 4600 b753 0e36 9791 4c87 4860 56a9
ad71 4717 eebc 3dc3 633e.

Step (7c):

W' = 0525 c5ba f6f9 78b1 1fd6 6e86 0de3 ebd3 314e
efb0 9ca7 8193 3b2e cb5f 8046 1b46 a87a 727a a317
e163 9dc4 2b55 8202 65dd 0f2c ce4d 57fe 84dc 08f5
49ee 896a a897 c29a dabb e0c6 78fe 0be5 753d 0d97
0d99 f3d2 1eef b822 7715 39e7 402d 63da 03d4 b66f
3789 066e 4c36 d025 3466 1b6a e359 f290 bb21 c1fc
01fe 23fb 0135 77d8 0ea9.

Iteration 5:

Step (1):

r = 0d2c cc3f 814b a506 7753 4948 8ba7 c8de 8a06
8da8 2eba 8b9f fc7e ab4f f439 8317 91b0 2700 28c8
c170 e8ec 16ca f279 08ba de15 912f dbf4 0562 0b1d
f95b b16e b24a 2b46 e0d7 e466 c636 684b e07d d57f
c67b e66d 6b16 af88 d873 047a 94e1 be1c 639f 2426
efb5 614b fbeb 00c4 d6af 0d14 0ac6 d54f c632 f933
80e6 e94d 5a35 675f fa6d.

W = 23d8 0778 c35c eccb b47f 8d83 881d 5e18 dfb8
a4e7 33af e9c8 af80 ef7b e6c0 a9b5 3d3c a4f3 524b
f72c 18b6 edb7 ba71 4523 9d48 4463 a817 9f18 83cf
71e9 96dc da61 58a2 3936 91bf 133b fdfe e906 b713
64b6 cdef 8446 2be2 8634 67d0 0f78 7a67 9ba4 b42f
92d1 ea7d 8c5e bfb9 8b7f d049 3907 61a8 1300 a9d1
4e18 cf4b dc08 064a ddcb.

Step (3):

$d_1, d_2, ..., d_5$ = 0, 1, 2, 1, 0.

Step (5):

D = 1061 f560 095a f8d8 81ae 7844 aa56 62cd d651
4c40 4f1a 4cb1 ebc3 0672 7ccc 4c10 0ded 8447 e1b0
5611 7135 78f3 86fd 6251 59ef 5755 c26f 7780 9fa9
a601 d059 b755 4cf9 bfa8 f491 6ce4 96c1 c082 c9d9
8622 b035 4341 3171 fa8c 6be3 c07a 418c b828 02f3
05a2 6998 40dc a632 ef9c a5a8 c9b3 e81e 902d 6699
4c00 4efa 3ce2 766d 42c1.

Step (7c):

W' = 23d8 0778 c35c eccb b47f 8d83 881d 5e18 dfb8
a4e7 33af e9c8 af80 ef7b e6c0 a9b5 3d3c a4f3 524b
f72c 18b6 edb7 ba71 4523 9d48 4463 a817 9f18 83cf
71e9 96dc da61 58a2 3936 91bf 133b fdfe e906 b713
64b6 cdef 8446 2be2 8634 67d0 0f78 7a67 9ba4 b42f
92d1 ea7d 8c5e bfb9 8b7f d049 3907 61a8 1300 a9d1
4e18 cf4b dc08 064a ddcb.

C.1.3 Example with public exponent $2^{16}+1$

C.1.3.1 Parameter selection

In this example the public verification exponent v is $2^{16}+1 = 65537$, which is odd. Therefore the secret prime factors p and q must satisfy:

$$\gcd(p-1, v) = \gcd(q-1, v) = 1.$$

p = b843 ab40 c311 80cd 1063 f5d6 2158 bc6d 9c93
b2fc 1def 7dfd 3152 a695 89d9 4a80 1000 bfee fb62
7321 5552 2138 61d2 39a1.

q = a8a1 c635 9063 d197 15a0 8e5f cd38 d6f2 3530
dde0 7359 2a67 1d02 e72a bb8e 8be2 599e 5bc8 ab53
c780 7d5e 9fd8 f680 5f79.

The public modulus n is 767 bits long.

n = 7960 d99c 1822 9f2c 2607 75d2 2eae 9941 6942
b3e8 f5ad c612 cd3f c529 70ed a698 0ba2 6388 08bd
b5cb c048 d63a 82d4 ac95 b166 9c43 4135 d7fc 19e2
022e a465 6bcc ee9b 7dba d90e 1125 91a2 1a66 1494
f4f6 e2b5 ce43 3b6a f390 79a0 2b48 c63f fc19.

$k_s = 766$.

The accreditation authority's private accreditation exponent u is the least positive integer satisfying: $uv+1$ is a multiple of $\text{lcm}(p-1, q-1)$.

u = 02f8 d0c5 e0fe bd5a fd60 b80d 24c0 cdab d657
4b19 c1cf 8c1c 05be 86a5 ff1d 3289 0d2f e009 57fd
727d 6cab 3138 f989 c4e2 aa1d f4dd a901 f518 c560
7fa7 1ea7 4893 535e 1d2a a178 949a 0c25 cc59 25a6
25d6 337e 24c7 af7a 6fff 6d42 f61c d3ff 8dff.

$m = 1$, $t = 1$

C.1.3.2 Identity selection

The identification data consists of $m = 1$ part. This identity part is constructed using the string 'Alex Ample' postfixed with a 16 bit field number.

I_{A1} = 416c 6578 2041 6d70 6c65 0001

C.1.3.3 Accreditation generation

J_{A1} = 3341 276c 2465 f078 5e20 9341 2a6d fe70 276c
2465 ee00 e301 9341 276c 2465 f078 5e20 9341 2a6d
fe70 276c 2465 ee00 e301 9341 276c 2465 f078 5e20
9341 2a6d fe70 276c 2465 ee00 e301 9141 276c 2465
f078 5e20 9341 2a6d fe70 276c 2465 ee00 e316.

C_{A1} = 2c61 c981 f375 ed78 5a4e 9939 e054 c63a 3809
8f2f f525 ed20 2d4e 0a65 f7af 7548 80ce 954f 8f15
a1e0 bb73 9cbb 815c 5970 4f1c 4e3e 7552 dd1c 4966
d352 1992 149d f30c be32 d1c7 569b 40e4 8b7d b558
b003 95b8 2ec1 c1e6 3ed3 cfd9 abe0 22de 827c.

C.1.3.4 Authentication exchange

Iteration 1:

Step (1):

r = 3a2c 36ef 335d b967 a76d b60f 7ad0 a6ea 518a
fcae 23d1 5ef3 3ead 463e 89af aa30 7a57 b5eb e1f5
b4aa 952e 125b 18be ac2f 245d f716 45e5 baee 9c5c
2750 4a76 92ac 0a45 bdd6 89a1 322f 6fa6 46d9 e18d
deb9 c948 e791 50cf 0776 104b 6f1d e369 977a.

W = 22b6 a130 b77d 5ace 0eaf b6e6 d55f 3eab d710
cd08 184d df53 6cd1 0372 b0da 7f34 97cf 9355 87c1
c877 072d e166 c09f 6f3e 1b21 4952 6be0 774c e4fb
a38f f58b ddd6 5595 ec51 1e1f 7da2 5677 a22a 9e3d
6f45 23cf 1927 ac1e 76ff 6614 0d46 9f2d 44de.

Step (3):

d_1 = 003d.

Step (5):

D = 1749 15ce a8cf cabb 678b 32d2 2424 c8fa 636e
cdca 7918 f47f b631 7741 e35e d84f 9257 bcd0 b8f6
27bc 7db4 b852 032b 8dea 028c 3681 a15c fedc ede8
8094 77c1 bec8 def4 c768 c78e 05f4 327e c58c c0f7
8229 8616 f15f 819b 746d 0efb 4747 9581 b39d.

Step (7c):

W' = 22b6 a130 b77d 5ace 0eaf b6e6 d55f 3eab d710
cd08 184d df53 6cd1 0372 b0da 7f34 97cf 9355 87c1
c877 072d e166 c09f 6f3e 1b21 4952 6be0 774c e4fb
a38f f58b ddd6 5595 ec51 1e1f 7da2 5677 a22a 9e3d
6f45 23cf 1927 ac1e 76ff 6614 0d46 9f2d 44de.

C.2 Mechanism based on discrete logarithms

C.2.1 Example using 768-bit p, 128-bit q and RIPEMD-128

C.2.1.1 Parameter selection

This example uses a 768-bit prime number p, a 128-bit prime number q (a prime factor of $p-1$), and RIPEMD-128 as the hash-function.

The 768-bit prime number p:

p = d716599e b22836ac fb221d0a f4c66b16 e3dceaee
a73a17fb aaa33c07 6cf3571f 54d89d49 38d7c311
e24b98f1 e510599d b53f7387 0d2acf2f 8fbf8267
c1df4fe3 2e8a04e4 14125c5f d6d8efd7 8c5f1563
4288cd6a 0caaf4cd 3cf44434 d7ea8143.

The 128-bit prime number q, a prime factor of $(p-1)$[1]:

q = a73a17fb aaa33c07 6cf3571f 54d89d49.

The element of order q in Z_p:

g = 5c7af3fa beff6338 f3137b85 a83e557b 49135e47
ba7ed438 e34b1fa0 af8c2651 15cf8b2f 3c924b33
0addf043 10ee6c41 a378541f 69a370dc b09f898a
f3204864 8a8433be cdb55d5d 6cdbc85d b6f3a654
0df8b209 1a674d77 cdee3e1e 86d4fb93.

C.2.1.2 Key selection

The 128-bit private key of entity A:

z_A = f1d4e85a eff74310 53adcac0 a9c155ce.

The 768-bit public verification key of entity A ($y_A = g^{z_A} \bmod p$):

y_A = 813eba80 bdbfdc78 15d09f74 ec21e1a6 4bd1a3c6
7a2591b2 44d53e2b 0c4dcb54 d5e2a8db 411e7c04
566d2671 12e72695 4a3c7699 a304255e fc58390c
b0566240 66ee9d2b 131ebbca 7217f973 86dcab2b
d4fb346c a2b5da9d 80954a65 4fa6f3c6.

C.2.1.3 Authentication exchange

Step (1):

Entity A selects a random number r.

r = 868b4b13 017364b7 e7dda29e cda55473.

$W = g^r \bmod p$
= 6ae62a6 d172be24 85830f5c c1524f4c a23172a8
c8691011 759f63d7 86b1a7d7 a6809f43 512f42c6
a6a444d6 a437f62f 02881f99 6e3638b0 93f6da41
cd4860e2 fb856e58 1a2cafed 8af85e6c 856ad852
c5f90648 915498bc d47fe84a 621c7bf3.

Step (2):

$h(W)$ = f084606b 90de7902 2bb16d2f 31996976.

Entity A sends $h(W)$ to entity B (Token$AB_1 = h(W)$).

Step (3):

Entity B chooses at random an integer d. (This example uses a 16-bit d.)

d = d47c.

Step (4):

Entity B sends challenge d to entity A.

Step (5):

Entity A computes the response D as $D = r - dz_A \bmod q$.

D = 1edee4bc 1667f13a 7cbf9d28 c5a356ea.

Step (6):

Entity A sends Token$AB_2 = D$ to entity B.

Step (7):

Entity B checks that $0 < D < q$, and calculates $W' = (y_A)^d g^D \bmod p$.

$(y_A)^d \bmod p$ = 6e6f703d ace31e6f 335f556b 42b24a6d
21771d60 2fa448be b74ae11d 3b63ff2f cecf2452
1417d470 04839f4a b15e91fa 72bbebfb 9b9c4b41
8c0c6a2d ef4a40e1 9a4a629c 32e63a0e fb03ec80
d55efeb8 173c6b26 58d28216 3be0ca6a 2d90cae6.

$g^D \bmod p$ = 8e249ba6 f0ef2f8a 156c0851 0bf23a2f
3408b9c0 7ec733cc dcfe78cf ca3bf160 7217be06
ccd9abc5 a392c7e7 4823070c 2e7c310a b26523a7
af58361c a685c3bb 1cd38f91 15479db1 cf38f7c8
852a4644 14cdc936 797e6883 7106bcb6 d1bbeaf1.

W' = 6ae62a6 d172be24 85830f5c c1524f4c a23172a8
c8691011 759f63d7 86b1a7d7 a6809f43 512f42c6
a6a444d6 a437f62f 02881f99 6e3638b0 93f6da41
cd4860e2 fb856e58 1a2cafed 8af85e6c 856ad852
c5f90648 915498bc d47fe84a 621c7bf3.

If $h(W') = h(W)$, then authentication for entity A is complete.

C.2.2 Example using 1024-bit p, 160-bit q and SHA-1

C.2.2.1 Parameter selection

This example uses a 1024-bit prime number p, a 160-bit prime number q (a prime factor of $p-1$), and Dedicated

[1] Note that p has been chosen so that a copy of q is embedded within p. Such an approach to the choice of p may be useful in situations where storage space and/or communications bandwidth is at a premium

Hash-Function 3 (also known as SHA-1), specified in clause 9 of ISO/IEC 10118–3, as the hash-function.

The 1024-bit prime number p:

p = ea9b8f92 26d7b2f6 729122ef 53ce81e2 567acf40
a7db660e ba5e4daf cb0ebc3a ccb15c36 896f67f0
703e7c69 afc4c24b 221a8968 5cdcfb3e 086d8f95
702cbfc5 8e4170a2 e10df7b5 2bf8f015 c5a689ca
48df291b e796c443 f5e7ad19 8c159f0a ba9d962e
60d34840 77b5993e 48bbc3ed fef5f54c accde46e
69a3f1f6 1ae08af9.

The 160-bit prime number q, a prime factor of $(p-1)$[1]:

q = cb0ebc3a ccb15c36 896f67f0 703e7c69 afc4c24b.

The element of order q in Z_p:

g = 26324f69 934e6733 c66367a5 af5a08d8 455a5125
29882857 b20083e8 f72420a9 1f16a377 6dc612ff
e652a2dd 05d51441 5f52c591 e8aa3127 8309ce2b
ca9e5b73 5e8cc526 0dc1608d 91f32a8d 31265adc
f2f2ff5f a4a786ef 25086bdb 061355cd 96ea33f6
429aef56 bc0c0aba db1ec3e0 b1140687 d60678c6
205c7f6d 6a236f87.

C.2.2.2 Key selection

The 160-bit private key of entity A:

z_A = 87146299 068b4b13 017364b7 e7dda29e cda5547e.

The 1024-bit public verification key of entity A ($y_A = g^{z_A} \bmod p$):

y_A = 819b36e6 62ddc4af 146dcf3a f888d61b 560ea5ea
8bb368f7 0e822e95 ef5e45c6 68b98732 725d29dc
21bf1394 29d95de2 98a6d595 9a7188c3 ab4b5d6d
20ca1d9e d6bc4d7a d23a4e3b 48cbe4ac da28d927
922c85ff db7e1f59 71a17dd5 dc68725c 32cf50f0
be5d8a73 f93bf113 1c55bf51 35b314be 5067fd31
9867041d 4c96e5cf.

C.2.2.3 Authentication exchange

Step (1):

Entity A selects a random number r.

r = 87146299 068b4b13 017364b7 e7dda29e cda5547a.

$W = g^r \bmod p$
= 397ad6f9 b435b01b 4c43a2d1 008ddade 1a086c2f
0ea25134 ff5a8653 a374dfbf 47f1a543 fbb58232
0357cce1 33aeb861 6aebd4b7 65dea271 0dff3a09
7c40602b 7e719499 0e9c7717 0ce73286 930e9e27
f8053b28 d2c80fd2 ec529839 27f34f46 bb9842b0
bd9c6405 1b2c58d8 c5cdcc50 69c4a430 d0f93cd0
6f2f75f3 298684f6.

Step (2):

$h(W)$ = d3cf43cd 80f2525d 360bf266 d11590de
7efdb987.

Entity A sends $h(W)$ to entity B (Token$AB_1 = h(W)$).

Step (3):

Entity B chooses at random an integer d. (This example uses a 40-bit d.)

d = a2 cda554a6.

Step (4):

Entity B sends the challenge d to entity A.

Step (5):

Entity A computes the response D as $D = r - dz_A \bmod q$.

D = 354bf25c 5f0e8cca f2aea2b9 7716a2d5 cb8ceb7e.

Step (6):

Entity A sends Token$AB_2 = D$ to entity B.

Step (7):

Entity B checks that $0 < D < q$, and calculates $W' = (y_A)^d g^D \bmod p$.

$(y_A)^d \bmod p$ = d95931d9 4ecd8e38 0993cf3d 9ab03767
abc0a08b 69a82166 83f73785 b940610f 9293ee53
be9e717f 6fd6a9be f7b0c140 1f374427 86856c96
c168f499 86800ecc 91f12765 be056ecb 7d03ce6b
4334a4d1 29cd1829 6705f4a6 105752c9 31190fe4
1a65c010 be4537f7 6913d471 50441aab 387a7e55
86e1debd 6343703f fd0eeef7.

$g^D \bmod p$ = c40924be 47db63b6 c48734a5 dd2f8a01
dc6c08ed 6cbfeda2 81b64230 fbbde7f8 fbddbd3e
e64d6887 014b5b0a 78c0d111 c6550c01 01f00536
304bc91d 7efe0c1e f9dede7b 004534e0 74347241
b430ba21 bd1c2f93 903860b7 d1a14716 cc541c51
ade947ef 827e6a27 78d67db6 2b4db4ba 918ef0f8
7ccca628 f3042268 25988779.

W' = 397ad6f9 b435b01b 4c43a2d1 008ddade 1a086c2f
0ea25134 ff5a8653 a374dfbf 47f1a543 fbb58232
0357cce1 33aeb861 6aebd4b7 65dea271 0dff3a09
7c40602b 7e719499 0e9c7717 0ce73286 930e9e27
f8053b28 d2c80fd2 ec529839 27f34f46 bb9842b0
bd9c6405 1b2c58d8 c5cdcc50 69c4a430 d0f93cd0
6f2f75f3 298684f6.

If $h(W') = h(W)$, then authentication for entity A is complete.

[1] Note that p has been chosen so that a copy of q is embedded within p. Such an approach to the choice of p may be useful in situations where storage space and/or communications bandwidth is at a premium

C.3 Mechanism based on a trusted public transformation

C.3.1 Example using 767-bit RSA and RIPEMD-160

C.3.1.1 Parameter selection

This example uses RSA as the asymmetric encipherment system, and Dedicated Hash-Function 1 (also known as RIPEMD-160), specified in clause 7 of ISO/IEC 10118-3, as the hash-function.

We suppose that A uses a 767-bit RSA modulus $n = pq$, a public RSA exponent e, and a private RSA exponent s, where:

p = cef2 8973 ddff 2ad1 ba38 4a98 71e0 7de1 d8ad 973f e2e1 2d6d 357c 19b2 7304 79b6 5c7e 6369 9a25 bb49 9f41 e7de 0f6f a105.

q = 9327 da68 0aa9 a22f 201b 429a acf1 de30 382f cb01 cf3d 6b4b 85a1 fa3c f851 4738 5100 09ee 7dad 2b4c 4673 0971 a417 41ad.

n = 76f5 7c6f 1d53 742a 45a2 1dab b9ca 6f4c eb1c 2317 6b02 9967 9ba4 3305 2c42 3146 44a3 9a79 5b57 5979 0685 8a10 932c f80d 8973 ecb6 30bf bc18 29db ff50 adf2 4465 a87c d236 1e8a 16c5 34f7 7acf ce94 0f59 234d c833 d279 0ade e26e 395f 71c5 1561.

e = 4d97 cc58 6e72 3582 ae31 9d48 5814 05f5 4e74 1737 6710 f052 acda 8fd5 1827 b485 d762 c713 4bda b4bd 08d6 7f78 4a5c 174e d35b 5ff9 62eb 1965 6af3 a353 4635 e843 89a0 78f0 e042 e656 ff35 0236 33f4 cc86 fcbd 4349 7c0d 3c19 7d20 fc60 bc91 1017.

s = 678a a11c 459c bd6d 10b9 9555 675a 7d7c 7850 af9b dc56 fe01 8846 7529 d02e 4aa6 85d0 3d2e 0e8e c027 ba69 3b4c f4dc 48c0 f2ad 74a2 25c4 fc38 ec52 94e4 a222 d922 7d53 389c c95f 9410 2b00 5840 247b ea8c 7a1f 3c60 ac3a 7297 704c 36e2 afbb e107.

A's public encipherment transformation is $P_A(r) = r^e \pmod{n}$.

C.3.1.2 Authentication exchange

Step (1):

Entity B chooses a random value r.

r = adec c15b d356 b0cd 1b74 9469 b421 ac9d 28ee 96a5 85ec 6284 9cc2 8beb 0e59 4c9f 7377 f151 18fc a3df 249a b0aa ebb0 cf35 91f6 7858 d8a0 16e4 40bf ee20 bbcf da92 8e09 6e2a a6ec eccd f7f1.

B computes $h(r)$, $r||h(r)$ and the challenge $d = P_A(r||h(r))$.

$h(r)$ = 4bc6 0e2c bfcb 238a 4d88 8b5f 3d4a eb02 3c16 1893.

$r||h(r)$ = adec c15b d356 b0cd 1b74 9469 b421 ac9d 28ee 96a5 85ec 6284 9cc2 8beb 0e59 4c9f 7377 f151 18fc a3df 249a b0aa ebb0 cf35 91f6 7858 d8a0 16e4 40bf ee20 bbcf da92 8e09 6e2a a6ec eccd f7f1 4bc6 0e2c bfcb 238a 4d88 8b5f 3d4a eb02 3c16 1893.

$d = P_A(r||h(r))$ = 60bd 94a5 7b0e 2eb9 0afb 5e21 630b 763f 8771 3479 98ed 4df6 3c9f bbf1 2369 d117 1c81 9277 63b9 3d5f 2af2 6288 7ee8 b24f b9d4 db2e c206 99b6 eb8f 2b31 3944 27e0 1f74 d501 cfca d45f 25ab dfd1 b605 c640 7d1a 597e 204a 1183 4670 c6b8 c52c 7cc3.

Step (2):

B sends d to A.

Step (3):

A performs the following computational steps.

(a) A recovers r and $h(r)$ by calculating

$$r||h(r) = S_A(d) = d^s \pmod{n}.$$

(b) A recomputes $h(r)$ from the value of r recovered in the previous step, and compares it with the value of $h(r)$ recovered in the previous step.

Given that the values of $h(r)$ agree, A sets $D = r$.

Step (4):

A sends D to B.

Step (5):

B compares D with r.

C.3.2 Example using 1024-bit RSA and SHA-1

C.3.2.1 Parameter selection

This example uses RSA as the asymmetric encipherment system, and Dedicated Hash-Function 3 (also known as SHA-1), specified in clause 9 of ISO/IEC 10118-3, as the hash-function.

We suppose that A uses a 1024-bit RSA modulus $n = pq$, a public RSA exponent e, and a private RSA exponent s, where:

p = d329 dc1d 1156 1582 b2ec b9c3 90e8 5588 0e0e 5a6b 96b8 8e0f 8fe2 1a1c 6dd2 0d86 c85b 3932 1fdb f85d 713d aaae ad1c dab1 3571 c6d1 80a5 c0e7 7159 1be0 e4ad 54ad.

q = bbb7 9564 0e4b 12d0 6c4a bfe3 1a93 f5f4 c69e 419f eac3 3c6c 2eaf e28e a60b eb6c 81c5 7477 1092 e8b2 67c3 6176 1969 cf37 1f26 60ad e102 6c5e c1c7 f394 6fa3 f72f.

n = 9ad7 01ef 79b2 6383 a98d 4995 5bc1 3684 c32a
60c6 8690 09a7 dd06 92f8 0914 7408 83d2 183b 851d
829b dbef 4da5 a973 9e83 e9e0 bb0f 7656 05cf 878e
03c9 0cda 6456 16e4 5a3b 8da2 4bfa 5a98 a00d ba3c
e534 fb9d 021c 8408 01a9 5b27 2f05 a989 73a9 35fb
6cef 475e 64ab d367 8caf 7abc 2025 4ffb 432f dbfb
a1dc 07ab 0805 25ac 76c3.

e = 4884 6170 eda8 4d88 0f9a 4755 06a1 6d09 7a9e
2c35 bbae 5ad8 07ff 91bf b832 8d8e 5c87 fcfb 92c7
cb22 752f 0af4 d2c4 8565 6410 f17c 3a8d cf92 8260
e490 75d5 9e0f 890e 9c41 02dc 2d3f 57c8 7a38 d145
24f9 cb28 4a12 70a3 9773 a759 a5ba f356 a871 79f6
4543 dcb9 eeb8 d224 6033 a5a1 2c01 46ac f66e 73a8
057d 4622 eb35 8649 d9eb.

s = 8076 3fa4 ced3 052c 4e60 6a0f 4be0 336c c5c7
1a9d df78 0fd4 adc7 8493 b106 e65e 6524 7d1e de7e
1bb1 312c 2d38 aa8a 3cb2 16dd d6ed ed3b 177e 17a2
9592 82ac 4bba be1d 0e2e 0762 6e77 739e 1d70 0896
5b28 de8b 525e c1f0 a7d4 6c15 0781 a4e7 b9a3 9d2d
9ca4 2a12 8174 aed3 35c4 9e7b 4da3 3e3b c55c e416
d27f a89f 07f1 d5f7 0423.

A's public encipherment transformation is $P_A(r) = r^e \pmod{n}$.

C.3.2.2 Authentication exchange

Step (1):

Entity B chooses a random value r.

r = fedb ad50 6bb5 2e55 e951 de0d a780 954e f6df
e7a3 2c4e 859e 5dae c493 1670 afc2 84e3 37cf 3963
b13f e614 e089 77c8 2062 3ceb 2cd4 fc2f 7ec4 aeaf
e48a 189a e6b2 516e 2b92 c4ea f516 48da e4c4 28a8
17ce 373a 40dc 9109 e255 f3e7 34d7 b1eb b03c 8a6c
cb8a 2f80 4a0d 1e8a.

B computes $h(r)$, $r||h(r)$, and the challenge $d = P_A(r||h(r))$.

$h(r)$ = cb70 5374 99ae 42c3 1c03 0777 af95 b0a6 d978
8684.

$r||h(r)$ = fedb ad50 6bb5 2e55 e951 de0d a780 954e
f6df e7a3 2c4e 859e 5dae c493 1670 afc2 84e3 37cf
3963 b13f e614 e089 77c8 2062 3ceb 2cd4 fc2f 7ec4
aeaf e48a 189a e6b2 516e 2b92 c4ea f516 48da e4c4
28a8 17ce 373a 40dc 9109 e255 f3e7 34d7 b1eb b03c
8a6c cb8a 2f80 4a0d 1e8a cb70 5374 99ae 42c3 1c03
0777 af95 b0a6 d978 8684.

$d = P_A(r||h(r))$ = 0e3d ad30 9d9e 5556 a4bd 7bab f749
a7ba c2a5 f350 fa23 07f2 72d7 8bd7 078e d5fe e00a
410c 0807 fd2c 5570 4cd3 d5db 8902 7640 0e8b 7b75
3c7c 26c1 faf4 7acc 75b0 daa7 c567 1823 d778 f432
b8a6 4457 2be2 9569 0f41 dc40 4abf e733 7b4b 2092
3d14 6ed5 9fdc d094 bd03 e5e9 8d9b 215e 7775 497b
0caf 43a7 7b85 f5eb c0eb d5b8 05cf.

Step (2):

B sends d to A.

Step (3):

A performs the following computational steps.

(a) A recovers r and $h(r)$ by calculating

$$r||h(r) = S_A(d) = d^s \pmod{n}.$$

(b) A recomputes $h(r)$ from the value of r recovered in the previous step, and compares it with the value of $h(r)$ recovered in the previous step.

Given that the values of $h(r)$ agree, A sets $D = r$.

Step (4):

A sends D to B.

Step (5):

B compares D with r.

Annex D
(informative)
Comparison of the mechanisms

This annex provides a comparison of the mechanisms specified in clauses 5, 6, and 7.

D.1 Measures for comparing the mechanisms

The following measures will be employed for the comparison: the computational complexity, the communication complexity, and the size of the claimant's accreditation information.

For some implementations, the claimant may use a portable device (e.g. a smart card) to prove the legitimacy of his accreditations to the verifier. In such implementations, the complexity of computation and communication for the smart card, and the storage in the smart card required for the claimant's accreditation information may be crucial, since the processing and storage capacities of smart cards are very limited in comparison with those allowed for the verifier. As reported in [9], in 1996 technology the clock rate is 10MHz at the most; RAM and EEPROM capacities range from 76 to 512 bytes and from 2 to 20 kbytes, respectively. If insufficient attention is paid to those features of the mechanisms stated in this annex, these factors will harm the effectiveness of the implementation.

Thus, this annex focuses on the complexity of the computations carried out by the claimant, the complexity of communications between the claimant and the verifier, and the storage in the smart card required for retaining the claimant's accreditation information.

In addition, the possibility of an attacker impersonating the claimant is considered in this annex. Specifically, an attacker who does not know the claimant's accreditation information may try to impersonate the claimant by generating witnesses based on guessed challenges, and the probability of success of this attack will be evaluated.

The following symbols are used.

C_P	Complexity of comPutation.
C_M	Complexity of comMunication.
S	required Storage size in a smart card.
P	Probability of succeeding in impersonating.

D.2 Mechanism based on identities

The mechanism is evaluated under two different assumptions on the values for the parameters n, v, t, m, corresponding to the Fiat-Shamir scheme ($v = 2$) and the Guillou-Quisquater scheme ($v > 2, t = m = 1$).

D.2.1 The case where v is large (e.g. the Guillou-Quisquater scheme)

D.2.1.1 Computational complexity

In this sub-clause, the particular case where v is large is considered. In particular, [5] provides a scheme with $\lfloor \log_2 v \rfloor \geq 16$.

By definition, the claimant carries out the following two computations for each iteration:

$$W = r^v \bmod^* n$$

and

$$D = r \prod_{i=1}^{m} \left({C_{A_i}}^{d_i} \right) \bmod^* n.$$

The following symbols are used in this clause.

N_W — the number of modular multiplications required to calculate W.

N_D — the number of modular multiplications required to calculate D.

$\mu(k)$ — the computational complexity of a modular multiplication with a k-bit long modulus.

It is known (see, for example, [6]) that there exists an effective algorithm for modular multiplication such that:

$$\mu(k) = O(k^{\log_2 3})$$

The following relation holds:

$$C_P = t(N_D + N_W)\mu(\lfloor \log_2 n \rfloor)$$

In the remaining part of this subclause, N_W and N_D are evaluated.

Using the 'right to left' version of the square and multiply algorithm for modular exponentiation, see [6] and [8], calculating ($r^v \bmod n$) requires computing the $\lfloor \log_2 v \rfloor$ values:

$$r^{2^1}, \cdots, r^{2^{\lfloor \log_2 v \rfloor}}$$

Then, W is given by

$$W = (r^1)^{b_0}(r^2)^{b_1} \cdots (r^{2^{\lfloor \log_2 v \rfloor}})^{b_{\lfloor \log_2 v \rfloor}} \bmod n$$

where b_i denotes the ith bit of the binary representation of v (b_0 is the least significant bit and $b_{\lfloor \log_2 v \rfloor}$ is the most significant bit).

For general v, half of the b_i's ($i = 0, \cdots, \lfloor \log_2 v \rfloor - 1$) will be zero, and therefore the value of N_W, is:

$$N_W = \frac{3}{2} \lfloor \log_2 v \rfloor .$$

If a similar method is used for calculating D, N_D is asymptotically given by:

$$N_D \approx \frac{3m}{2} \lfloor \log_2 v \rfloor .$$

Therefore, C_P is given by:

$$C_P \approx \frac{3t}{2}(m+1) \lfloor \log_2 v \rfloor \mu(\lfloor \log_2 n \rfloor).$$

In particular, in the case $t = m = 1$, which is known as the Guillou-Quisquater scheme, we have:

$$C_P \approx 3 \lfloor \log_2 v \rfloor \mu(\lfloor \log_2 n \rfloor).$$

D.2.1.2 Communication complexity

In each iteration, the claimant sends Token$AB_1 = W$ and Token$AB_2 = D$ to the verifier, which are both ($\lfloor \log_2 n \rfloor + 1$) bits long. The verifier also sends a challenge, a sequence of m bit-strings, each of which is ($\lfloor \log_2 v \rfloor + 1$) bits long. Since m is negligible in comparison with $\lfloor \log_2 n \rfloor$, the following holds:

$$\begin{aligned} C_M &= t\{2(\lfloor \log_2 n \rfloor + 1) + m(\lfloor \log_2 v \rfloor + 1)\} \\ &\approx t(2\lfloor \log_2 n \rfloor + m \lfloor \log_2 v \rfloor). \end{aligned}$$

In the case of the Guillou-Quisquater scheme, we have:

$$C_M \approx 2\lfloor \log_2 n \rfloor + \lfloor \log_2 v \rfloor .$$

The claimant is also allowed to send Token $AB_1 = h(W \| \text{Text})$ instead of Token $AB_1 = W$. In this case, C_M is:

$$C_M \approx t(\lfloor \log_2 n \rfloor + H + m \lfloor \log_2 v \rfloor)$$

where H is the number of bits in a hash-code for the hash-function h.

D.2.1.3 Size of the claimant's accreditations

The claimant retains private accreditation information $C_{A_1}, C_{A_2}, \cdots, C_{A_m}$ in addition to the public key pair (v, n). Thus, the storage in bits required for this is

$$S \approx (m+1)\lfloor \log_2 n \rfloor + \lfloor \log_2 v \rfloor .$$

In the case of the Guillou-Quisquater scheme, we have:

$$S \approx 2\lfloor \log_2 n \rfloor + \lfloor \log_2 v \rfloor .$$

D.2.1.4 Degree of security

An attacker, who does not know the claimant's accreditation information, may try to impersonate the claimant by generating witnesses after guessing challenges to be sent by the verifier. The attacker will succeed in impersonating the claimant with probability

$$P = \frac{1}{v^{tm}}.$$

In the case of the Guillou-Quisquater scheme, we have:

$$P = \frac{1}{v}$$

D.2.2 Fiat-Shamir scheme

In this subclause, the particular case $v = 2$ is considered. For this case the mechanism is known as the Fiat-Shamir scheme.

D.2.2.1 Computational complexity

Since $v = 2$, we have $\lfloor \log_2 v \rfloor = 1$, and hence

$$N_W = 1,\ N_D = \frac{m}{2}.$$

Therefore,

$$C_P = \frac{1}{2} t(m+2)\mu(\lfloor \log_2 n \rfloor).$$

D.2.2.2 Communication complexity

Since m is negligible in comparison with $\lfloor \log_2 n \rfloor$,

$$C_M \approx 2t \lfloor \log_2 n \rfloor .$$

The claimant is also allowed to send Token $AB_1 = h(W \| \text{Text})$ instead of Token $AB_1 = W$. In this case, C_M is:

$$C_M \approx t(\lfloor \log_2 n \rfloor + H)$$

where H is the number of bits in a hash-code for the hash-function h.

D.2.2.3 Size of the claimant's accreditations

$$S \approx (m+1)\lfloor \log_2 n \rfloor .$$

D.2.2.4 Degree of security

The probability of an attacker guessing all mt challenges successfully is:

$$P = \frac{1}{2^{mt}}$$

D.3 Certificate-based mechanism using discrete logarithms

D.3.1 Computational complexity

The computations that the claimant carries out are

$$W = g^r \bmod p$$

and

$$D = r - dz_A \bmod q.$$

Since the complexity of computing D is negligible in comparison with that for W, the total complexity C_P is given by:

$$C_P \approx \frac{3}{2}\lfloor \log_2 q \rfloor \mu(\lfloor \log_2 p \rfloor).$$

D.3.2 Communication complexity

The claimant sends Token$AB_1 = W$ and Token$AB_2 = D$ to the verifier, which are $(\lfloor \log_2 p \rfloor + 1)$ and $(\lfloor \log_2 q \rfloor + 1)$ bits long, respectively. The verifier sends a challenge, which is $(\lfloor \log_2 q \rfloor + 1)$ bits long. Therefore:

$$C_M \approx \lfloor \log_2 p \rfloor + 2\lfloor \log_2 q \rfloor.$$

The claimant is also allowed to send Token $AB_1 = h(W\|\text{Text})$ instead of Token $AB_1 = W$. In this case, we have:

$$C_M \approx H + 2\lfloor \log_2 q \rfloor$$

where H is the number of bits in a hash-code for the hash-function h.

D.3.3 Size of the claimant's accreditations

The claimant needs to store the private key z_A in addition to the three positive integers p, q, and g. Therefore

$$S \approx 2(\lfloor \log_2 p \rfloor + \lfloor \log_2 q \rfloor).$$

D.3.4 Degree of security

A challenge d is chosen from the set $\{0, 1, \cdots, q-1\}$. Therefore, the probability of an attacker guessing a challenge successfully is:

$$P = \frac{1}{q}.$$

D.4 Certificate-based mechanism using an asymmetric encipherment system

For the purposes of this discussion it is assumed that the RSA cryptosystem is the asymmetric encipherment system. The following notation is used

a) (y_A, n) is the claimant's public key.

b) z_A is the claimant's private key, that is, the relation $y_A z_A \equiv 1 \pmod{\lambda(n)}$ holds.

c) $P_A(m) = m^{y_A} \bmod n$.

d) $S_A(c) = c^{z_A} \bmod n$.

D.4.1 Computational complexity

The computation carried out by the claimant is:

$$S_A(d) \overset{?}{=} d^{z_A} \bmod n.$$

Therefore, the computational complexity is:

$$C_P \approx \frac{3}{2}\lfloor \log_2 n \rfloor \mu(\lfloor \log_2 n \rfloor).$$

D.4.2 Communication complexity

The verifier sends a challenge $P_A(r\|h(r))$, which is $(\lfloor \log_2 n \rfloor + 1)$ bits long, whilst the claimant sends Token$AB = r$ back to the verifier. Supposing that $\lfloor \log_2(r\|h(r)) \rfloor \approx \lfloor \log_2 n \rfloor$, the length in bits of TokenAB is $\lfloor \log_2 n \rfloor - \lfloor \log_2 h(r) \rfloor$. Therefore:

$$C_M \approx 2\lfloor \log_2 n \rfloor - H$$

where H is the number of bits in a hash-code for the hash-function h.

D.4.3 Size of the claimant's accreditations

The claimant retains the accreditation information, which is the RSA private key pair (z_A, n). Its length in bits is:

$$S \approx 2\lfloor \log_2 n \rfloor.$$

D.4.4 Degree of security

The probability that an attacker succeeds in guessing the value of r is:

$$P = \frac{1}{2^{\lfloor \log_2 n \rfloor - H}}.$$

D.5 Comparison of the mechanisms

Table 1 summarises the parameters discussed in D.2–D.4.

Table 2, on the other hand, gives a comparison of the mechanisms when certain concrete values are specified for the parameters of the mechanisms (e.g. $\lfloor \log_2 n \rfloor$, $\lfloor \log_2 v \rfloor$, $\lfloor \log_2 p \rfloor$). Each value in Table 2 is the ratio of the evaluated values for one of the mechanisms to the corresponding value for the Fiat-Shamir scheme.

The following specific choices for parameters have been made to obtain the figures quoted in Table 2.

— *Fiat-Shamir scheme (FS).* The values $m = 2$ and $t = 10$ are assumed, as Fiat and Shamir, [3], recommend.

— *Fiat-Shamir scheme with hashed commitments (FSH).* This case is the case where Token $AB_1 = h(W\|\text{Text})$. As a number of existing hash-functions generate 128-bit hashes, H is set to 128. The values for the other parameters are the same as those for Fiat-Shamir, see above.

— *Guillou-Quisquater scheme (GQ).* The value $\lfloor \log_2 v \rfloor = 16$ is assumed.

— *Schnorr scheme (SC).* The values $\log_2 p = 512$ and $\log_2 q = 140$ are recommended by Schnorr, [10].

— *Guillou-Quisquarter scheme with hashed commitments (GQH).* This is the case where Token $AB_1 = h(W \| \text{Text})$. As a number of existing hash-functions generate 128-bit hashes, H is set to 128. The values for the other parameters are the same as those for GQ, see above.

— *Certificate-based mechanism using an asymmetric encipherment system (RSA).* As a number of existing hash-functions generate 128-bit hashes, H is set to 128.

	C_P	S	C_M	P
FS	$(1/2)t(m+2)\mu(\lfloor \log_2 n \rfloor)$	$(m+1)\lfloor \log_2 n \rfloor$	$2t\lfloor \log_2 n \rfloor$	$1/2^{mt}$
FSH	$(1/2)t(m+2)\mu(\lfloor \log_2 n \rfloor)$	$(m+1)\lfloor \log_2 n \rfloor$	$t(\lfloor \log_2 n \rfloor + H)$	$1/2^{mt}$
GQ	$3\lfloor \log_2 v \rfloor \mu(\lfloor \log_2 n \rfloor)$	$2\lfloor \log_2 n \rfloor + \lfloor \log_2 v \rfloor$	$2\lfloor \log_2 n \rfloor + \lfloor \log_2 v \rfloor$	$1/v$
GQH	$3\lfloor \log_2 v \rfloor \mu(\lfloor \log_2 n \rfloor)$	$2\lfloor \log_2 n \rfloor + \lfloor \log_2 v \rfloor$	$\lfloor \log_2 n \rfloor + H + \lfloor \log_2 v \rfloor$	$1/v$
SC	$(3/2)\lfloor \log_2 q \rfloor \mu(\lfloor \log_2 p \rfloor)$	$2(\lfloor \log_2 p \rfloor + \lfloor \log_2 q \rfloor)$	$\lfloor \log_2 p \rfloor + 2\lfloor \log_2 q \rfloor$	$1/q$
SCH	$(3/2)\lfloor \log_2 q \rfloor \mu(\lfloor \log_2 p \rfloor)$	$2(\lfloor \log_2 p \rfloor + \lfloor \log_2 q \rfloor)$	$H + 2\lfloor \log_2 q \rfloor$	$1/q$
RSA	$(3/2)\lfloor \log_2 n \rfloor \mu(\lfloor \log_2 n \rfloor)$	$2\lfloor \log_2 n \rfloor$	$2\lfloor \log_2 n \rfloor - H$	$2^{H - \lfloor \log_2 n \rfloor}$

Table 1 — Evaluation functions

	C_P	S	C_M	P
FS	1	1	1	1
FSH	1	1	0.625	1
GQ	3	0.67969	0.10195	1
GQH	3	0.67969	0.0644531	1
SC	10.5	0.75781	0.077344	2^{-120}
SCH	10.5	0.75781	0.0398437	2^{-120}
RSA	38.4	0.66667	0.0875	2^{-364}

Table 2 — Evaluation ratios for specific parameter choices

Annex E
(informative)
Information about Patents

During the preparation of this part of ISO/IEC 9798, information was gathered concerning relevant patents upon which application of this part of ISO/IEC 9798 might depend. Relevant patents were identified as shown in the table below. However, ISO/IEC cannot give authoratitive or comprehensive information about the validity or scope of patents.

The identified patent-holders have stated that licences will be granted in appropriate terms to enable application of this part of ISO/IEC 9798, provided that those who seek licences agree to reciprocate.

Further informtion is available from the identified patent-holders.

Area	Inventors	Patent #	Issue data	Contact address
Fiat-Shamir identification	Shamir-Fiat	US 4,748,668	1988-05-31	News Digital Systems Ltd. Stoneham Rectory Stoneham Lane Eastleigh Hampshire SO50 9NW, UK
Schnorr signatures	Schnorr	US 4,995,082	1991-02-19	RSA Data Security Inc. Director of Licensing 2955 Campus Drive, Suite 400 San Mateo, CA 94403-2507 USA
GQ identification	Guillou-Quisquater	US 5,140,634	1992-08-18	CCETT Patent and IPR office BP 59, 4 Rue du Clos Courtel F-35512 Cesson Sévigné, France
		EP 0,311,470	1992-12-16	Philips International B.V. Corporate Patents and Trademarks P.O. Box 220 5600 AE Eindhoven The Netherlands

Annex F
(informative)
Bibliography

[1] J. Brandt, I. Damgard, P. Landrock and T. Pedersen, *Zero-knowledge authentication scheme with secret key exchange*, in: 'Advances in Cryptology — CRYPTO '88', S. Goldwasser (editor), Springer-Verlag, Berlin (1990), pp. 583–588.

[2] U. Feige, A. Fiat and A. Shamir, *Zero knowledge proofs of identity.* Journal of Cryptology, Volume 1 (1988) pp. 77–94.

[3] A. Fiat and A. Shamir, *How to prove yourself: Practical solutions to identification and signature problems*, in: 'Advances in Cryptology — CRYPTO '86', A.M. Odlyzko (editor), Springer-Verlag, Berlin (1987), pp. 186–194.

[4] S. Goldwasser, S. Micali and C. Rackoff, *The knowledge complexity of interactive proof systems.* SIAM Journal on Computing, Volume 18 (1989) pp. 186–208.

[5] L.C. Guillou and J.-J. Quisquater, *A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory*, in: 'Advances in Cryptology — EUROCRYPT '88', C.G. Günther (editor), Springer-Verlag, Berlin (1988), pp. 123–128.

[6] D.E. Knuth, *The Art of Computer Programming, Volume 2.* Addison-Wesley (2nd edition, 1981).

[7] C.H. Lim and P.J. Lee, *A key recovery attack on discrete log based schemes using a prime order subgroup*, in: 'Advances in Cryptology — Crypto '97', Lecture Notes in Computer Science 1294, Springer-Verlag, Berlin (1997), pp. 249–263.

[8] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of applied cryptography.* CRC Press, Boca Raton (1997).

[9] D. Naccache, D. M'Raihi, *Cryptographic smart cards.* IEEE Micro, Volume 16 no.3 (June 1996).

[10] C.P. Schnorr, *Efficient identification and signatures for smart cards*, in: 'Advances in Cryptology — CRYPTO '89', G. Brassard (editor), Springer-Verlag, Berlin (1990), pp. 239–252.

ICS 35.040

Price based on 29 pages

37

INTERNATIONAL
STANDARD

ISO/IEC 11770-1

First edition
1996-12-15

Information technology — Security techniques — Key management —

Part 1:
Framework

Technologies de l'information — Techniques de sécurité —
Partie 1: Cadre général

Reference number
ISO/IEC 11770-1:1996(E)

Contents

ISO/IEC Copyright Office • Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Annexes

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 11770-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 27, *IT Security techniques.*

ISO/IEC 11770 consists of the following parts, under the general title *Information technology — Security techniques — Key management:*

- *Part 1: Framework*
- *Part 2: Mechanisms using symmetric techniques*
- *Part 3: Mechanisms using asymmetric techniques*

Further parts may follow.

Annexes A to E of this part of ISO/IEC 11770 are for information only.

Introduction

In Information Technology there is an ever increasing need to use cryptographic mechanisms for the protection of data against unauthorised disclosure or manipulation, for entity authentication, and for non-repudiation functions. The security and reliability of such mechanisms are directly dependent on the management and protection afforded to a security parameter, the key. The secure management of these keys is critical to the integration of cryptographic functions into a system, since even the most elaborate security concept will be ineffective if the key management is weak. The purpose of key management is to provide procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic mechanisms.

The fundamental problem is to establish keying material whose origin, integrity, timeliness and (in the case of secret keys) confidentiality can be guaranteed to both direct and indirect users. Key management includes functions such as the generation, storage, distribution, deletion and archiving of keying material in accordance with a security policy (ISO 7498-2).
This part of 11770 has a special relationship to the frameworks for Open System Security (ISO/IEC 10181). All the frameworks, including this one, identify the basic concepts and characteristics of mechanisms covering different aspects of security. This part of ISO/IEC 11770 introduces general models for key management that are fundamental for symmetric and asymmetric cryptographic mechanisms.

Information technology — Security techniques — Key management —

Part 1:
Framework

1 Scope

This part of ISO/IEC 11770:

1. identifies the objective of key management;
2. describes a general model on which key management mechanisms are based;
3. defines the basic concepts of key management common to all the parts of this multi-part standard;
4. defines key management services;
5. identifies the characteristics of key management mechanisms;
6. specifies requirements for the management of keying material during its life cycle; and
7. describes a framework for the management of keying material during its life cycle.

This framework defines a general model of key management that is independent of the use of any particular cryptographic algorithm. However, certain key distribution mechanisms may depend on particular algorithm properties, for example, properties of asymmetric algorithms.

Specific key management mechanisms are addressed by other parts of ISO/IEC 11770. Symmetric mechanisms are addressed in part 2 (ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*). Asymmetric mechanisms are addressed in part 3 (ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*). This part of ISO/IEC 11770 contains the material required for a basic understanding of parts 2 and 3. Examples of the use of key management mechanisms are included in ISO 8732 and ISO 11166. If non-repudiation is required for key management, ISO/IEC 13888 should be used.

This part of ISO/IEC 11770 addresses both the automated and manual aspects of key management, including outlines of data elements and sequences of operations that are used to obtain key management services. However it does not specify details of protocol exchanges that may be needed.

As with other security services, key management can only be provided within the context of a defined security policy. The definition of security policies is outside the scope of this multi-part standard.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 11770. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 11770 are encouraged to investigate the possibility of applying the most recent edition of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards

ISO 7498-2: 1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture.*

ISO/IEC 9798-1: 1991, *Information technology — Security techniques — Entity authentication mechanisms — Part 1: General model.*

ISO/IEC 10181-1: 1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview.*

3 Definitions

The following terms are used as defined in ISO 7498-2:

data integrity

data origin authentication

digital signature

The following term is used as defined in ISO/IEC 9798-1:

entity authentication

The following terms are used as defined in ISO/IEC 10181-1:

security authority

security domain

trusted third party (TTP)

For the purposes of ISO/IEC 11770, the following definitions apply.

3.1 asymmetric cryptographic technique: A cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

3.2 certification authority (CA): A centre trusted to create and assign public key certificates. Optionally, the certification authority may create and assign keys to the entities.

3.3 decipherment: The reversal of a corresponding encipherment.

3.4 encipherment: The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data.

3.5 key: A sequence of symbols that controls the operation of a cryptographic transformation (e.g., encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

3.6 key agreement: The process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key.

3.7 key confirmation: The assurance for one entity that another identified entity is in possession of the correct key.

3.8 key control: The ability to choose the key, or the parameters used in the key computation.

3.9 key distribution centre (KDC): An entity trusted to generate or acquire, and distribute keys to entities that each share a key with the KDC.

3.10 keying material: The data (e.g., keys, initialisation values) necessary to establish and maintain cryptographic keying relationships.

3.11 key management: the administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

3.12 key translation centre (KTC): An entity trusted to translate keys between entities that each share a key with the KTC.

3.13 private key: That key of an entity's asymmetric key pair which should only be used by that entity.

NOTE: A private key shall not normally be disclosed.

3.14 public key: That key of an entity's asymmetric key pair which can be made public.

3.15 public key certificate: The public key information of an entity signed by the certification authority and thereby rendered unforgeable.

3.16 public key information: information specific to a single entity which contains at least the entity's distinguishing identifier and at least one public key for this entity. There may be other information regarding the certification authority, the entity, and the public key included in the public key information, such as the validity period of the public key, the validity period of the associated private key, or the identifier of the involved algorithms.

3.17 random number: A time variant parameter whose value is unpredictable.

3.18 secret key: A key used with symmetric cryptographic techniques and usable only by a set of specified entities.

3.19 sequence number: A time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period.

3.20 symmetric cryptographic technique: A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

3.21 time stamp: A time variant parameter which denotes a point in time with respect to a common time reference.

3.22 time variant parameter: A data item used by an entity to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp.

4 General Discussion of Key Management

Key management is the administration and use of the services of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material.

The objective of key management is the secure administration and use of these key management services and therefore the protection of keys is extremely important.

Key management procedures depend on the underlying cryptographic mechanisms, the intended use of the key and the security policy in use. Key management also includes those functions that are executed in cryptographic equipment.

4.1 Protection of Keys

Keys are a critical part of any security system that relies on cryptographic techniques. The appropriate protection of keys depends on a number of factors, such as the type of application for which the keys are used, the threats they face, the different states the keys may assume, etc. Primarily, depending upon the cryptographic technique, they have to be protected against disclosure, modification, destruction and replay. Examples of possible threats to keys are given in Annex A. The validity of a key shall be limited in time and amount of use. These constraints are governed by the time and amount of data required to conduct a key-recovery attack and the strategic value of the secured information over time. Keys that are used to generate keys need more protection than the generated keys. Another important aspect of the protection of keys is avoidance of their misuse, e.g., use of a key encipherment key to encipher data.

4.1.1 Protection by Cryptographic Techniques

Some threats to keying material can be countered using cryptographic techniques. For example: encipherment counters key disclosure and unauthorised use; data integrity mechanisms counter modification; data origin authentication mechanisms, digital signatures, and entity authentication mechanisms counter masquerade.

Cryptographic separation mechanisms counter misuse. Such separation of functional use may be accomplished by binding information to the key. For example: binding control information to the key assures that specific keys are used for specific tasks (e.g. key encipherment, data integrity); key control is required for non-repudiation using symmetric techniques.

4.1.2 Protection by non-Cryptographic Techniques

Time stamps may be used to restrict the use of keys to certain valid time periods. Together with sequence numbers, they also protect against the replay of recorded key agreement information.

4.1.3 Protection by Physical Means

Each cryptographic device within a secure system usually needs to protect the keying material it uses against the threats of modification, deletion and, except for public keys, disclosure. The device typically provides a secure area for key storage, key use and cryptographic algorithm implementation. It may provide the means

- to load keying material from a separate secure key storage device,
- to interact with cryptographic algorithms implemented in separate *smart* security facilities (for example, smart cards, memory cards), or
- to store keying material off-line (for example, on diskette).

Secure areas typically are protected by physical security mechanisms.

4.1.4 Protection by Organisational Means

One means of protecting keys is to organise them into key hierarchies. Except at the lowest level of the hierarchy, keys in one level of a hierarchy are used solely to protect keys in the next level down. Only keys in the lowest level of the hierarchy are used directly to provide data security services. This hierarchical approach allows the use of each key to be limited, thus limiting exposure and making attacks difficult. For example, the compromise of a single session key is limited to compromising only the information protected by that key.

The use of secure areas addresses the threats of key disclosure, modification and deletion by unauthorised entities. However, the threat remains that system administrators, authorised to perform certain management functions on components of the key management service, may misuse the special access privileges they possess. In particular, they might try to obtain a master key (a top level key in a key hierarchy). Disclosure of a master key will potentially enable the possessor to discover or manipulate all other keys protected by it (i.e. all other keys in that particular key hierarchy). It is therefore desirable to minimise access to this key, perhaps by arranging that no single user has access to its value. Such a requirement can be met by dividing the key (dual control or even n-times control) or using dedicated cryptographic schemes *(Secret Sharing Schemes).*

4.2 Generic Key Life Cycle Model

A cryptographic key will progress through a series of states that define its life cycle. The three principal states are:

Pending Active: In the Pending Active state, a key has been generated, but has not been activated for use.

Active: In the Active state, the key is used to process information cryptographically.

Post Active: In this state, the key shall only be used for decipherment or verification.

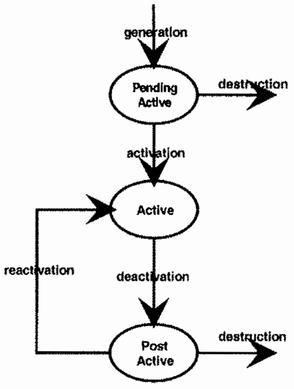


Figure 1 — Key Life Cycle

NOTE: The user of a Post Active key shall be assured that the data had been cryptographically processed before the key became Post Active. This assurance is commonly provided by a trusted time variant parameter.

A key that is known to be compromised shall become Post Active immediately and may require special handling. A key is said to be compromised when its unauthorised use is known or suspected.

Figure 1 shows these states and the corresponding transitions.

Figure 1 represents a generic life cycle model. Other life cycle models may have additional details that may be substates of the three states presented. The majority of life cycles require an archival activity. This activity may be associated with any of the states, depending on the particular details of the life cycle.

4.2.1 Transitions between Key States

When a key progresses from one state to another it undergoes one of the following transitions as also depicted in figure 1:

Generation is the process of generating a key. Key Generation should be performed according to prescribed key generation rules; the process may involve a test procedure to verify whether these rules have been followed..

Activation makes a key valid for cryptographic operations.

Deactivation limits a key's use. This might occur because the key has expired or has been revoked.

Reactivation allows a Post Active key to be used again for cryptographic operations.

Destruction ends a key's life cycle. It covers logical destruction of the key and may also involve its physical destruction.

Transitions may be triggered by events such as the need for new keys, the compromise of a key, the expiration of a key, and the completion of the key life cycle. All these transitions include a number of services for key management. The relationships between the transitions and the services are shown in Table 1. These services are explained in Clause 5.

Any particular cryptographic approach will only require a subset of the services offered in Table 1.

4.2.2 Transitions, Services and Keys

Keys for particular cryptographic techniques will use different combinations of services during their life cycles. Two examples are given below.

For symmetric cryptographic techniques, following the generation of a key, the transition from Pending Active to Active includes key installation and may also include key registration and distribution. In some cases, installation may involve the derivation of a specific key. The lifetime of a key should be limited to a fixed period. Deactivation ends the Active state, usually upon expiration. If compromise of a key in the Active state is suspected or known, revocation also causes it to enter the Post Active state. A Post Active key may be archived. If an archived key is needed again, it will be reactivated and may need to be installed or distributed again before it is fully active. Otherwise, following deactivation, the key may be deregistered and destroyed.

For asymmetric cryptographic techniques, a pair of keys (public and private) is generated and both keys enter the Pending Active state. Note that the life cycles of the two keys are related but not identical. Before it enters the Active state, a private key may optionally be registered, may optionally be distributed to its user and is always installed. The transitions between the Active and the Post Active states for a private key, including deactivation, reactivation, and destruction, are similar to those described above for symmetric keys. When a public key is certified, commonly a certificate containing the public key is created by the CA, to assure the validity and ownership of the public key. This public key certificate may be placed in a directory or other similar service for distribution, or may be passed back to the owner for distribution. When the owner sends out information signed with his private key he may add his certificate. The key pair becomes active when the public key is certified. When a key

Table 1 — Transitions and Services

Transition	Service	Notes
Generation	generate-key	mandatory
	register-key	optional either here or activation
	create-key-certificate	optional
	distribute-key	optional
	store-key	optional
Activation	create-key-certificate	optional
	distribute-key	optional
	derive-key	optional
	install-key	mandatory
	store-key	optional
	register-key	optional either here or generation
Deactivation	store-key	optional
	archive-key	optional either here or destruction
	revoke-key	optional
Reactivation	create-key-certificate	optional
	distribute-key	optional
	derive-key	optional
	install-key	mandatory
	store-key	optional
Destruction	deregister-key	mandatory, if registered
	destroy-key	mandatory
	archive-key	optional either here or deactivation

pair is used for digital signature purposes the public key may remain in the Active or Post Active state for an indefinite time after its related private key has been deactivated or destroyed. Access to the public key may be necessary to verify digital signatures made before the original expiration date of the associated private key. When asymmetric techniques are used for encipherment and the key used for encipherment has been deactivated or destroyed, the corresponding key of the pair may remain in the Active or Post Active state for later decipherment.

The use or application of a key may determine the services for that key. For example, a system may decide not to register session keys, since the registration process may last longer than their lifetime. By contrast, it is necessary to register a secret key when symmetric techniques are used for digital signature.

5 Concepts of Key Management

5.1 Key Management Services

This Clause describes a general structure for key management to aid understanding of the key management services, how they fit together and how they are supported.

Key management relies on the basic services of generation, registration, certification, distribution, installation, storage, derivation, archiving, revocation, deregistration and destruction. These services may be part of a key management system or be provided by other service providers. Depending on the kind of service, the service provider must fulfil certain minimum security requirements (e.g., secure exchange) to be trusted by all entities involved. For example, the service provider may be a trusted third party. Figure 2 shows that the key management

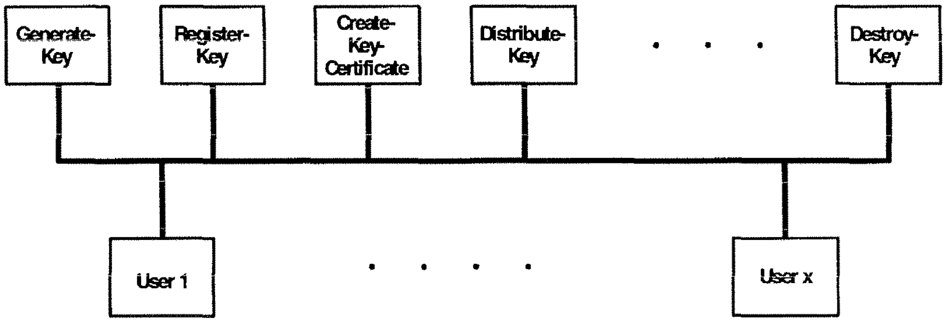


Figure 2 — Key Management Services

services are positioned at the same level and may be used by a variety of different users (persons or processes). These users may utilise different key management facilities within different applications, making use of services specific to their needs. The key management services are listed in Table 1.

5.1.1 Generate-Key

Generate-Key is a service that is invoked to generate keys in a secure way for a particular cryptographic algorithm. This implies that the key generation cannot be manipulated and, that the keys are generated in an unpredictable way and according to a prescribed distribution. This distribution is imposed by the cryptographic algorithm for which it will be used and the required level of cryptographic protection. The generation of some keys, e.g., master keys, demands special care because knowledge of these keys offers access to all related or derived keys.

5.1.2 Register-Key

The service Register-Key associates a key with an entity. It is provided by a registration authority, and is usually applied when symmetric cryptographic techniques are used. When an entity wishes to register a key it has to contact the registration authority. Key registration involves a request for registration and a confirmation of that registration.

A registration authority maintains a register of keys and related information in a suitably secure manner. Annex B offers details of key management information.

Operations provided by a key registration authority are registration and deregistration.

5.1.3 Create-Key-Certificate

The service Create-Key-Certificate assures the association of a public key with an entity and is provided by a certification authority. When a request for key certification is accepted, the certification authority creates a key certificate. Public key certificates are discussed in more detail in ISO/IEC 11770-3.

5.1.4 Distribute-Key

Key distribution is a set of procedures to provide key management information objects (see example in Annex B) securely to authorised entities. A specific case of key distribution is key translation where keying material is established between entities using a key translation centre (see Subclause 6.2). ISO/IEC 11770-2 offers different mechanisms to establish keys between entities. ISO/IEC 11770-3 includes mechanisms for key agreement of secret keys and transport mechanisms for secret and public keys.

5.1.5 Install-Key

The service Install-Key is always needed before the use of a key. The installation of the key means the establishment of the key within a key management facility in a manner that protects it from compromise.

5.1.6 Store-Key

The service Store-Key provides secure storage of keys intended for current or near-term use or for back-up. It is usually advantageous to provide physically separate key storage. For example, it ensures confidentiality and integrity for keying material or integrity for public keys. Storage may occur in all key states (i.e. Pending Active, Active and Post Active) of a key's life cycle. Depending on the importance of the keys, they can be protected using one of the following mechanisms:

- physical security (e.g., by storing them within a tamper-resistant device or by external means such as diskette or memory card),
- encipherment with keys that are themselves protected by physical security, or
- protecting the access to them by password or PIN.

For all keying material, any attempted compromise should be detectable.

5.1.7 Derive-Key

The service Derive-Key forms a potentially large number of keys using a secret original key called the derivation key, non-secret variable data and a transformation process (which also need not be secret). The result of this process is the derived key. The derivation key needs special protection. The derivation process should be non-reversible and non-predictable to ensure that the compromise of a derived key does not disclose the derivation key or any other derived key.

5.1.8 Archive-Key

Key archiving provides a process for the secure, long-term storage of keys after normal use. It may use the service of key storage but allows for a different implementation such as off-line storage. Archived keys may need to be retrieved at a much later date to prove or disprove certain claims after normal use is discontinued.

5.1.9 Revoke-Key

When the compromise of a key is suspected or known the service Revoke-Key assures the secure deactivation of the key. This service is necessary for keys having reached their expiration date. Revocation of keys will also take place when a key owner's circumstances change. After a key is revoked it may only be used for decipherment and verification. The service Revoke-Key is not appropriate to certificate based schemes, where key life is controlled by expiry of the certificate.

NOTE: Some applications use the term delete-key for this service

5.1.10 Deregister-Key

The service Deregister-Key is a procedure provided by a key registration authority that removes the association of a key with an entity. It is part of the destruction process (see 5.1.11 Destroy-Key). When an entity wishes to deregister a key, the registration authority is contacted.

5.1.11 Destroy-Key

The service Destroy-Key provides a process for the secure destruction of keys that are no longer needed. Destroying a key means eliminating all records of this key management information object, such that no information remaining after the destruction provides any means of recovering the destroyed key. This is taken to include the destruction of all archived copies. However, before archived keys are destroyed a check must be carried out to ensure that no archived material protected by these keys will ever be needed again.

NOTE: Some keys may be stored outside an electronic device or system. Destruction of those keys requires additional administrative measures.

5.2 Support Services.

Other services may be needed to support key management.

5.2.1 Key Management Facility Services

Key management services may make use of other services that are security related. These services include:

access control This service may be used to ensure that the resources of a key management system can be accessed only by authorised entities in an authorised manner.

audit The tracking of security-relevant actions that appear in a key management system. Audit trails may help identify security risks and security leaks.

authentication This service should be used to establish an entity as an authorised member of a security domain.

cryptographic services These services should be used by key management services to provide integrity, confidentiality, authentication and non-repudiation.

time service This service is necessary for generating time variant parameters such as validity durations.

5.2.2 User-oriented Services

Cryptographic systems and devices may require other services that are necessary for adequate functionality, e.g., user registration services. These services are implementation specific and beyond the scope of this part of ISO/IEC 11770.

6 Conceptual Models for Key Distribution

The distribution of keys between entities can be complex. It is influenced by the nature of the communications links, the trust relationships involved and the cryptographic techniques used. The entities may either communicate directly or indirectly, may belong to the same or different security domains, and may or may not use the services of a trusted authority. The following conceptual models illustrate how these different cases influence the distribution of keys and information.

6.1 Key Distribution between Communicating Entities

Communication between entities is influenced by the link between these entities, the trust between these entities and the cryptographic techniques used.

There exists a connection between entities A and B, who wish to exchange information using cryptographic techniques. This communication connection is illustrated in Figure 3. Generally, key distribution must take place over a secure channel that is logically different from the traffic channel.

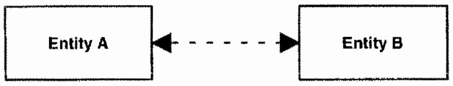


Figure 3 — Communications Link between Two Entities

Cases where direct communicating entities are involved are key agreement, key control and key confirmation. Further details of these cases are within Part 2 (ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*) and Part 3 (ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*) of ISO/IEC 11770.

6.2 Key Distribution within One Domain

The following model is based on the concept of a security domain with a security authority according to ISO/IEC 10181-1. This authority may offer key management services such as the translation of keys. When the entities use an asymmetric technique for the secure exchange of information, the following cases can be distinguished:

- For data integrity or data origin authentication, the recipient requires the sender's corresponding public key certificate.
- For confidentiality the sender requires a valid public key certificate of the recipient.
- For authentication, confidentiality, and integrity, each partner requires the public key certificate of the other. This provides the means for mutual non-repudiation.

Each entity may need to contact its authority to get an appropriate public key certificate. If the communicating partners trust each other and can mutually authenticate their public key certificates, then no authority is needed.

NOTE: There exist cryptographic applications where no authority is involved. In that situation the communicating partners may only securely exchange specific public information instead of their public key certificates.

When symmetric cryptography is in use between two such partners, key generation is initiated in one of two ways:

1. By one entity generating the key and sending it to a Key Translation Centre (KTC);
2. By one entity asking a Key Distribution Centre to generate a key for subsequent distribution.

If key generation is carried out by one of the entities, secure distribution of the key can be handled by a Key Translation Centre, as illustrated in Figure 4. The numbers represent the steps of the exchange. The KTC receives the enciphered key from entity A (1), deciphers it and re-enciphers it using the key shared between itself and entity B. Then it may

- either forward the enciphered key to entity B (2), or
- send it back to entity A (3), who forwards it to entity B (4).

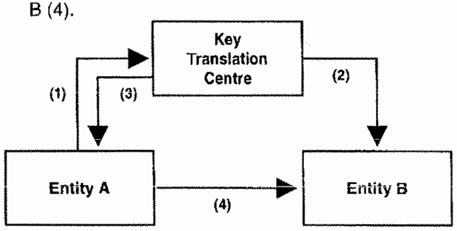


Figure 4 — Key Translation Centre

If key generation is carried out by a trusted third party, there are two options for subsequent distribution of the key to the communicating partners; these cases are illustrated in Figure 5 — Conceptual Model of a Key Distribution Centre — and Figure 6 — Key Distribution by Forwarding a Key from Entity A to Entity B.

Figure 5 illustrates the case in which the Key Distribution Centre is able to communicate securely with both entities. In this case, once a key has been generated at the request of one of the entities, the Key Distribution Centre is responsible for securely distributing the key to both entities. The request of the shared key is represented by (1) and the distribution of the key to the communicating partners by (2a) and (2b).

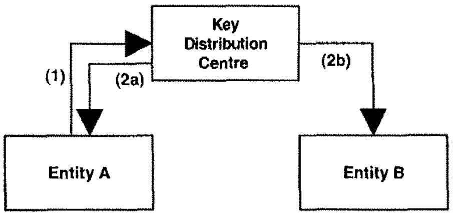


Figure 5 — Conceptual model of a Key Distribution Centre.

When only entity A asks for a secret key to be shared between entities A and B, the authority may act in two different ways. If it can securely communicate to both entities it may distribute the secret key to both of them as described above. If the authority can only communicate with entity A, entity A is responsible for distributing the key to entity B. Figure 6 illustrates this kind of key distribution. The request for a shared key is represented by (1) and the distribution to entity A by (2).The forwarding of this key from A to B is represented by (3).

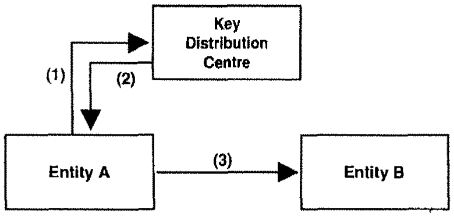


Figure 6 — Key Distribution by Forwarding a Key from an Entity A to Entity B

6.3 Key Distribution between Domains

The model here involves two entities named A and B belonging to two different security domains which share at least one cryptographic technique (i.e. symmetric or asymmetric). Each security domain has its own security authority: one trusted by A and one trusted by B. If A and B either trust each other or each trusts the authority of the other's domain, then keys are distributed according to Subclause 6.1 or 6.2.

Two cases can be distinguished for key establishment between A and B:

- the obtaining of the public key certificate of B (when applicable), and
- the establishment of a shared secret key between A and B.

Different key relationships are possible between these components. These key relationships reflect the nature of the trust between the components.

When the entities use an asymmetric technique for the exchange of information and do not have access to a common directory service that offers the public key certificates, each shall contact its respective authority to get its partner's public key certificate (see Figure 7 (1)). The authorities of A and B exchange the public key certificates of entities A and B (2) and forward them to A and B (3). Then A and B are able to communicate securely and directly (4).

A different approach for the exchange of public key certificates is cross-certification (see also Annex D).

When the entities communicate using a symmetric technique each entity also has to contact its respective authority securely (1) to receive a secret key that allows them to communicate. The authorities agree on a common secret key (2) to be used by the entities. One authority distributes the secret key to both entities using the other authority as a distribution centre. The latter authority may also provide key translation ((2) and (3)).

When only the entity A asks for a secret key for communication with entity B, the authority may act in two ways. If it can communicate to both entities it may distribute the secret key to both of them as described above. If the authority can only communicate with one entity, the entity receiving the key is responsible for forwarding the key to the other entity.

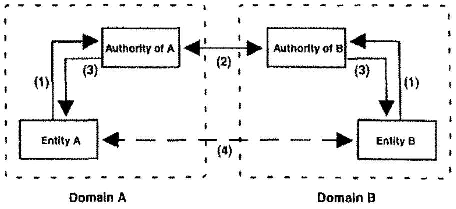


Figure 7 — Key Distribution between two Domains

Sometimes the authorities of A and B will have neither a mutual trust relationship nor a direct communications path. Then they shall involve an authority, X, whom they both trust as illustrated in Figure 8 (see arrows (2a) and (2b)). Authority X may generate a key and distribute it to the authorities of A and B (see arrows (3a) and (3b) in Figure 8). Alternatively, Authority X may forward a received secret key or public key certificate (for example (2a)) from the authority of A to the authority of B (3b). The authorities then have to forward the received key to their respective entities (see (4a) and (4b) in Figure 8) who may then exchange information securely (5). It may be necessary to seek successive authorities until a chain of trust is established.

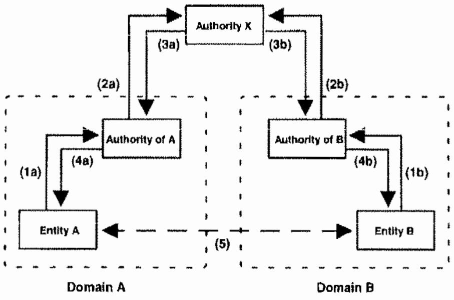


Figure 8 — Chain of Trust between Authorities

7 Specific Service Providers

Some of the services that a key management system requires may be provided by external service providers. Possible entities for services are:

- a Key Registration or Certification Authority,
- a Key Distribution Centre as defined in ISO/IEC 8732,
- a Key Translation Centre as defined in ISO/IEC 8732.

Annex A
(informative)

Threats to Key Management

Key management is susceptible to a number of threats. These include the following.

Disclosure of the keying material: Either the keying material is in plaintext, is not protected and can be accessed, or is enciphered and can be deciphered.

Modification of keying material: Changing the keying material so that it does not operate as intended.

Unauthorised deletion of keying material: Removal of the key or key related data.

Incomplete destruction of keying material: This may lead to the compromise of current or future keys.

Unauthorised revocation: The direct or indirect removal of a valid key or keying material.

Masquerade: The impersonation of an authorised user or entity.

Delay in executing key management functions: This may result in a failure to generate, distribute, revoke or register a key, a failure to update the key repository in a timely manner, in a failure to maintain a user's authorisation levels, and so on. The delay threat may result from any of the previously mentioned threats or from physical failure of the key related equipment.

Misuse of keys

- The use of a key for a purpose for which it is not authorised, e.g., the use of a key enciphering key for data encipherment.
- The use of a key management facility for a purpose for which it is not authorised, e.g., the unauthorised encipherment or decipherment of data.
- The use of a key after it has expired.
- Excessive use of a key.
- Provision of keys to an unauthorised recipient.

Annex B
(informative)

Key Management Information Objects

A key management information object consists of a key or keys, together with, optionally, other information that controls how the key(s) may be used. The control information may, rather than being explicit, be implied by conventions controlling the use of the key management information object. (For example, the use of one key of an asymmetric cipher pair is controlled by the agreed use of the other, one for encipherment and the other for decipherment.).

The control information may control the following:

- the type of object the key may protect (e.g., data or key management information object);
- valid operations (e.g., encipherment, decipherment);
- the allowed user;
- the environment in which the key may be used;
- other aspects particular to the specific control technique or application that uses the key management information object.

For the purposes of optimization the key management information object may be partially or wholly created within the key generation process.

A particular example of a key management information object is a key certificate. It contains at least the following signed by a certification authority:

- the keying material;
- the identity of the user who is able to use the corresponding key management information object;
- the operations which the corresponding key management information object performs (may be implicit);
- the period of validity;
- the identity of the certification authority.

The following ASN.1-definition is an example of a key management information object, although key management information objects may contain other, implementation specific parameters:

```
Key             ::=     PROTECTED   {KeyContents, protectionType};
KeyContents     ::=     SEQUENCE            {
                        keyID               [0]     Key_Identity,
                        keyValue            [1]     Key_Value,
                        checkValue          [2]     Check_Value,
                        cryptoMethod        [3]     Cryptographic_Method,
                        timeStamp           [4]     Time_Stamp,
                        generAuthority      [5]     Generating_Authority,
                        certiAuthority      [6]     Certification_Authority,
                        issuer              [7]     Issuer,
                        validity            [8]     Validity_of_Key};
```

It consists of the parameters Key_Identity (unambiguous identity), Key_Value (the value of the key) and Check_Value (a check sum to ensure integrity of the key) where only the Key_Value is mandatory. The parameters Cryptographic_Method, Issuer and Validity_of_Key control the use of the key in restricting it to specific algorithms for a limited time and a specific user. These parameters are important for the control of a key's use, but are optional. The parameters Generating_Authority, Certification_Authority and Time_Stamp are important for the proof of a key's origin and its age, but are also optional. For a key certificate the parameter Issuer is mandatory.

Annex C
(informative)
Classes of Cryptographic Applications

The common classification of cryptographic systems is defined by the two principal cryptographic techniques used, i.e. symmetric and asymmetric. Because key management must cater for both techniques another approach is needed. Therefore the following section classifies cryptographic systems according to the functionality provided by the technique.

In general, a cryptographic system offers two different types of cryptographic service: authentication services and encipherment services. Encipherment services are used to cryptographically protect information; i.e., they provide data confidentiality. Authentication services are primarily used for entity authentication, data origin authentication, data integrity and non-repudiation. The types of cryptographic systems and the corresponding operations are demonstrated in Figure C-1.

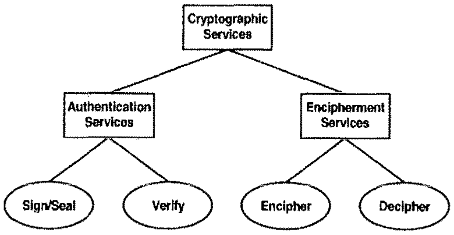


Figure C-1 — Cryptographic Services and Corresponding Mechanisms

C.1 Authentication Services and Keys

Authentication services provide for the authentication of communicating entities (entity authentication), for the authentication of the source of data (data origin authentication), for non-repudiation, and for data integrity. This service may make use of the following mechanisms:

seal a data unit which involves the production of a cryptographic check value of the data for data integrity, e.g., generate a message authentication code (MAC) with a symmetric algorithm.

sign a data unit which involves the generation of a digital signature for data origin authentication, data integrity and/or non-repudiation.

verify a sealed data unit which involves calculating a cryptographic check value of the data and comparing it with the referenced check value (proof of data integrity).

verify a signed data unit which involves the verification of a digital signature to determine whether it was produced by the claimed originator and/or the proof of data integrity.

Within the authentication service the signing and the sealing processes use information which is either private (i.e. unique and confidential) to the originator or secret and only known by the originator and the recipient; the verifying process uses either procedures and information that are publicly available but from which the originator's private information cannot be deduced or the shared secret of the originator and the recipient. The essential characteristic of signing is that the signature can only be produced using the originator's private information, his *private key.* Thus when the signature is verified by using the originator's *public key*, it can subsequently be proven to a third party (e.g., a notarisation authority) that only the unique holder of the private information could have produced the signature.

An authentication service uses two out of three types of keys:

sealing key a shared, *secret* key.

signature key a unique, *private* key that is associated with the originator.

verification key either a *public key* or a *secret key*.

For symmetric techniques an authentication service uses a sealing key and a verification key which are represented by the same secret key, for asymmetric techniques it uses the signature key and the verification key which are represented by a key pair consisting of a public and a private key.

C.2 Encipherment Services and Keys

Encipherment services primarily provide confidentiality of information but also data integrity. Depending on the technique used security services such as authentication and non-repudiation might be included. It makes use of two basic mechanisms:

encipher which produces ciphertext from the data it is given;

decipher which produces plaintext from the corresponding ciphertext.

An encipherment service may be characterised by the cryptographic technique used, i.e., symmetric or asymmetric. When using symmetric techniques the operations encipher and decipher are handled by the same key (shared secret key). When using asymmetric techniques the operations encipher and decipher are handled by two distinct but related keys, i.e., the public and the private key.

Annex D
(informative)
Certificate Lifecycle Management

This informative Annex describes the requirements and procedures as they apply to the management of the public key certificate lifecycle.

D.1 The Certification Authority

The CA is "trusted" by its subscribers. Such trust is based on the use of adequate cryptographic mechanisms and equipment, and on professional management and control practices. This trust shall be confirmed by an independent audit function (internal, external or both) which shall make the audit results available to subscribers.

The CA shall be responsible for:

1. Identifying the entities whose public key information is presented for certification.
2. Ensuring the quality of the asymmetric key pair used to produce public key certificates.
3. Securing the certification process and the private key used to sign the public key information.
4. Managing the system-specific data that are to be included into the public key information, such as public key certificate serial number, certification authority identification, etc.
5. Assigning and checking of validity periods.
6. Advising the entity identified in the public key information that a public key certificate has been issued. The means used to convey this advice shall be independent of the method used to convey the public key information to the CA.
7. Ensuring that two different entities are not assigned the same identity, so that they can be properly distinguished.
8. Maintaining and issuing of revocation lists.
9. Logging all steps involved in the public key certificate generation process.

One CA can certify another CA's public key information to provide a public key certificate. Hence, authentication may involve a chain of public key certificates. The first public key certificate in such a chain shall be obtained and authenticated by some means other than with public key certificates.

D.1.1 The CA's Asymmetric Key Pair

The CA shall have a secure key management facility that is able to generate the asymmetric key pair for use by that CA. The generation process shall ensure the unpredictability of the keying material. No opponent shall gain any advantage by knowledge of the generation process.

The CA's private key is used to sign the entity's public key information. Since its possession would enable an opponent to masquerade as the CA and generate forged public key certificates, it shall be given a high level of protection. Thus, the CA's private key shall be well protected when used inside the key management facility. It shall enter or leave the key management facility in a protected way and under the control of the CA itself.

The integrity of the CA's public verification key is essential to the security of the public key certificate system. If the CA's public key is not contained in a public key certificate, then special precautions shall be taken to ensure its authenticated distribution. At the user sites provision shall be taken to ensure the authenticity of the stored copy of the CA's public key.

The CA's public verification key is used to validate the public key certificates of other users. Before each use of the CA's public key, the user shall assure that the verification key is currently valid.

D.2 The Certification Process

This Clause describes requirements and procedures as they apply to the certification process.

D.2.1 Model for Public Key Certification

This Clause specifies a basic model for the certification of public keys. The model separates the main functions into logical entities (see Figure D-1):

1. Certification authority (CA): the entity responsible for certifying the public key information of a user entity.
2. Directory (DIR): the entity responsible for making the public key certificates available online for ready use by the user entities.
3. Key Generator (KG): the entity responsible for the generation of an asymmetric key pair.

4. Registration Authority (RA): the entity responsible for providing assured user identities to the CA.
5. User entity (A)

The relations between the logical entities of the model and the corresponding security requirements on these relations are discussed. The logical entities may be combined. For example, *A* and the KG may be combined when the user entity generates the asymmetric key pair itself, or, the CA and the KG may be combined if the CA generates the key pairs on behalf of the user entities.

NOTE: Care must be taken that a certificate generated by a combined RA and CA is the same as one produced by an RA and CA that are separate and distinct.

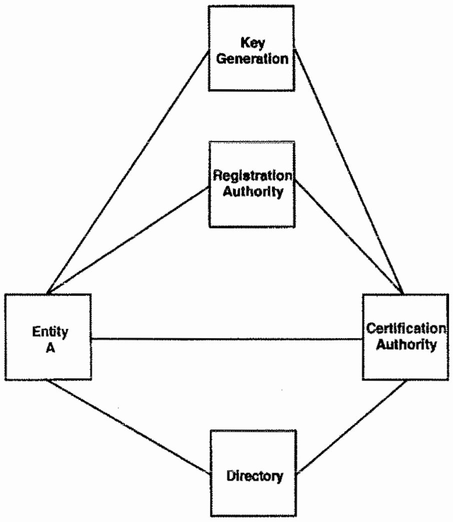


Figure D-1 — Basic Model for Public Key Certification

D.2.1.1 Certification Relations

This Clause describes some of the certification relations of the basic model and the corresponding security requirements. Not all relations need to be active in a particular system implementation. For instance the tasks of the RA, the CA and the KG may be combined.

A - KG Entity *A* requests the key generator KG to generate an asymmetric key pair. The KG is trusted to generate asymmetric key pairs of good quality. The KG generates the key pair (s_A,v_A), such that s_A is a signature key and v_A is a verification key and transfers it back to *A*. This transfer shall take place in an authenticated and confidential way. The KG and *A* shall be absolutely sure that any third party can neither modify the asymmetric key pair nor can read the values during the transfer.

A - RA Entity *A* requests registration by the Registration Authority RA. *A* shall submit its identity information to the RA. The RA verifies the authenticity of *A*'s information and possibly adds system-specific data. The information is then forwarded to the CA in a secure way.

A - CA Entity *A* requests the Certification Authority CA to certify its public key information (or a subset thereof) including its public key and its distinguished name. The submission of the public key information to the CA shall take place in a way that assures its authenticity and integrity. The CA verifies the authenticity of *A*'s public key information, possibly adds system specific data, and then signs the completed public key information to produce *A*'s public key certificate. The public key certificate may then be transferred back to *A*.

Upon reception of the issued public key certificate, *A* verifies its correctness using the public verification key v_{CA} of the certification authority. This public verification key v_{CA} shall be made available to *A* in an authenticated way. From that point on, *A*'s public key can be distributed as a public key certificate and be used by everybody who has access to the CA's public verification key.

If, however, the Certification Authority requests the KG to generate an asymmetric key pair on behalf of entity *A*, then A's key pair shall be transferred from the KG to *A*. The security requirements for the transfer are confidentiality, integrity, and authenticity. In addition, the CA is trusted to preserve the confidentiality, integrity and authenticity of all the asymmetric key pairs during processing and storage. Finally, the CA shall transfer *A's* private key to *A,* being absolutely sure that any third party can neither modify nor read the transferred value.

A - DIR Entity *A* transfers its public key certificate to the Directory DIR and registers it in the directory. Entity authentication and access control are required for registering the public key certificate in the directory. There shall be an agreement between *A* and DIR as to who is authorised to manage the entity's directory entry. In one application scenario, DIR manages all the directory entries. In a second application scenario, each entity *X* is responsible for and manages its own directory entry.

RA - CA RA requests the CA to certify *A*'s public key information. The transfer of *A*'s public key information from RA to CA shall take place in an authenticated way. The CA verifies the authenticity of *A*'s public key information, possibly adds system specific data, and then signs the completed public key information to produce *A*'s public key certificate. The CA advises the RA of the certification.

CA - KG The Certification Authority CA requests the key generator KG to generate an asymmetric key pair on behalf of entity *A*. The KG is trusted to generate asymmetric key pairs of good quality. The KG generates the key pair and transfers it back to the CA. This transfer shall take place in an authenticated and confidential way. The KG and the CA shall be absolutely sure that no third party can modify the asymmetric key pair nor can read the values during the transfer. The CA is trusted to preserve the confidentiality and authenticity of all the asymmetric key pairs during processing and storage.

CA - DIR The CA transfers the produced public key certificates directly to the Directory DIR and registers them in the directory. Entity authentication and access control are required for registering the public key certificates in the directory.

D.2.2 Registration

Registering an entity's key involves the submission of an entity's certificate request and its validation by the RA or the CA. The following subclauses illustrate the requirements as they apply to the submission of an entity's certificate request. The certificate request may or may not include the public key value.

D.2.2.1 Submission of an Individual's Certificate Request

For low risk applications, acceptance of certificate request should be based on identifying the individual applying for a public key certificate. The certificate requests do not have to be presented in person, but reasonable business practices are to be used for identifying the individual.

For high risk applications, acceptance of certificate request should be based on the appearance in person (or by an authorised agent) of the individual applying for the public key certificate, and the use of reasonable commercial standards to identify the person (and agent of that person if required). This may involve verification of the identity by a trusted third entity.

D.2.2.2 Submission of a Legal Entity's Certificate Request

Acceptance of the certificate request should be based on hand delivery of the certificate request information by at least one representative of the entity and:

1. The signature and seal (where applicable) on a letterhead authorizing the application for a public key certificate,
2. The use of reasonable commercial practices to identify the signature and seal (where appropriate) of the entity, and
3. The use of reasonable commercial practices to identify the representatives delivering the certificate request information.

D.2.3 Relationships between Legal Entities

There will be a requirement for legal entities to enter into contractual relationships with other legal entities. This may be accommodated in different ways:

1. The company officers have personal asymmetric key pairs. The legal entity acts as the CA for its company officers. Transactions are authorised by individuals using their personal keys certified by the company CA. Recipients check that the originator is certified by the company, whose public key, in turn, is certified by some higher CA.
2. The company officers do not have personal asymmetric key pairs. Only the legal entity has one or more asymmetric key pairs. Recipients check that the transactions are consistent with the company's public key. Recipients do not need to concern themselves with the authorisation privileges and policies of the originating company.

D.2.4 Certificate Generation

The public key certificate generation process shall take place before any use of the asymmetric key pair.

The following steps are needed in the certification generation process:

1. Checking the public key information for errors.
2. Accepting the public key information: Requirements for accepting public key information are specified in the Subclause on registration above.
3. Preparing and adding the data required for public key certificate management; optionally, the CA may generate the entities' asymmetric key pair(s).
4. Computing the signature for the public key certificate. This may involve a hash function.
5. The audit log entry. Actions of the CA in the public key certificate generation process shall be logged.

For high-risk applications it may be desirable to (1) require multiple signatures on the public key certificate by the CA, with the signatures being performed in independent cryptographic facilities (with different private keys), or to (2) require multiple signatures on the public key information by different CAs.

D.2.5 Renewal/Lifetime

A public key certificate has a lifetime that is indicated by a validity period stated in the public key certificate or is otherwise defined by the CA's management.

D.3 Distribution and Use of Public Key Certificates

This Clause describes the requirements and procedures as they apply to the distribution and use of public key certificates.

D.3.1 Distribution and Storage of Public Key Certificates

Once a public key certificate has been generated, no special measures need be taken to ensure its confidentiality or integrity. The public key certificates may be stored in a public directory for easy access of the users.

D.3.2 Verification of Public Key Certificates

To validate a public key certificate, the verifying entity *B* shall at least verify the CA's signature on the public key certificate. If the public key certificate has assigned a validity period, *B* shall assure that entity *A*'s public key information is currently valid (see also D.5 Certificate Revocation). To verify a public key certificate, the verifier shall possess of a valid copy of the CA's public verification key.

D.4 Certification Paths

Neither all CAs need to know and certify each other nor need there be a strict hierarchy of CAs. It will be likely that CAs certify each other (cross-certify) to allow a flexible use and exchange of public key certificates. This cross-certification should be done using high assurance levels and a careful code of practice. Once a network of cross public key certificates exists, validation paths of public key certificates can be constructed. A user only needs to have trust in the verification key of one CA. This trust then extends via the certification path to a partner's public key issued by an unknown CA.

D.5 Certificate Revocation

Certificates may be revoked before their scheduled expiration by the issuing CA. This may occur for a number of reasons, including the following:

1. compromise of the entity's private key,
2. request for cancellation by an entity,
3. change of affiliation of the entity,
4. termination of the entity,
5. false identification of the entity,
6. compromise of the CA's private key,
7. termination of the CA.

Accordingly, a procedure and means of rapid communication shall be in place to facilitate the secure and authenticated cancellation of:

1. one or more public key certificates of one or more entities,
2. the set of all public key certificates issued by a CA based on a single asymmetric key pair used by a CA to sign the public key information,
3. all public key certificates issued by a CA, regardless of asymmetric key pair function used.

The last two requirements provide the means to revoke public key certificates when a compromise or suspected compromise of the CA's private key occurs or when the asymmetric key pair used to sign the public key certificates is being changed. Whether public key certificates expire or are revoked, copies of old public key certificates shall be retained by a trusted third party for the time required by prudent business practice, law and regulations.

When a private key of an entity or a CA is cancelled for any reason, the CA issuing that public key certificate shall take immediate action to inform all entities in the system that any corresponding public key certificates have been revoked. This may for example take the form of a message authenticated by the CA and sent to all entities, a message authenticated by another CA, the maintenance of an on-line list of revoked public key certificates by a trusted third party or even publication of a list of revoked or valid public key certificates .

When a public key certificate is revoked because of a suspected or actual compromise of a private key, the private key shall not be used any more. The public key certificate shall be used only for verification purposes, provided that the data was signed before the time of the revocation. Furthermore any keying material enciphered by that public key certificate (without regard to type) shall be discontinued immediately.

When a public key certificate expires or is revoked for reasons other than actual or suspected compromise, the private key shall not be used any more. The public key certificate may still be used for verification or decipherment purposes. All keying material sent and protected by that public key certificate (without regard to type) should be replaced as soon as operationally convenient.

D.5.1 Revocation Lists

A revocation list contains a time-stamped list of serial numbers or public key certificate identifiers for those public key certificates that have been revoked by a CA. Two kinds of time-stamps can be used in a revocation list:

1. the date and time at which the CA issues the revocation,
2. the date and time of known or suspected compromise.

The latter date, when known, renders easier the auditing of suspected messages. A public key certificate remains on the revocation list at least until its expiration date. Time-stamping is critical, since it shall be known at what time the binding between an entity's public key and identity has been dissolved.

Once revocation has occurred for known or suspected compromise, information signed using the associated private key shall no longer be recognised as valid, if the signature was processed after the suspected date of compromise or if the date of signature cannot be reliably determined. Information shall not be enciphered using a revoked public key.

A revocation list shall be:

1. dated and signed by the CA so that entities can validate the integrity of the list and the date of distribution,
2. issued by the CA at regular intervals, even if no changes have occurred since the last issuance, and
3. accessible to all entities of the system except when precluded e.g., by law, regulation or court order.

A variety of distribution mechanisms is possible for revocation lists, including:

- delivery to each user as a message/transaction by a trusted third party,
- requests to a trusted third party by a user for the current status of a given public key certificate,
- queries to the CA for its current revocation list.

The CA shall publish and distribute a new revocation list periodically.

Annex E
(informative)

Bibliography

ISO 8732: 1988, *Banking — Key management (wholesale).*

ISO/IEC 9594-8: 1990, *Information technology — Open Systems Interconnection — The Directory — Part 8: Authentication framework.*

ISO/IEC 10116: 1991, *Information technology — Modes of operation for an n-bit block cipher algorithm.*

ISO 11166-1: 1994, *Banking — Key management by means of asymmetric algorithms — Part 1: Principles, procedures and formats.*

ISO 11568-1: 1994, *Banking — Key management (retail) — Part 1: Introduction to key management.*

ISO 11568-2: 1994, *Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers.*

ISO 11568-3: 1994, *Banking — Key management (retail) — Part 3: Key life cycle for symmetric ciphers.*

ISO 11568-4[1]: *Banking — Key management (retail) — Part 4: Key management techniques for public key cryptosystems.*

ISO 11568-5[1]: *Banking — Key management (retail) — Part 5: Key life cycle for public key cryptosystems.*

ISO/IEC 11770-2: 1996, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques.*

ISO/IEC 11770-3[1]: *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques.*

ISO/IEC 13888[1]: *Information technology — Security requirements — Non-repudiation* (all parts).

[1] To be published

ICS 35.040

Descriptors: data processing, information interchange, protection of information, security techniques, key management, cryptography.

Price based on 21 pages

INTERNATIONAL STANDARD

ISO/IEC 11770-2

First edition
1996-04-15

Information technology — Security techniques — Key management —

Part 2:
Mechanisms using symmetric techniques

Technologies de l'information — Techniques de sécurité — Gestion de clés —

Partie 2: Mécanismes utilisant des techniques symétriques

Reference number
ISO/IEC 11770-2:1996(E)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

International Standard ISO/IEC 11770-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Sub-committee SC 27, *IT Security techniques.*

ISO/IEC 11770 consists of the following parts, under the general title *Information technology - Security techniques - Key management:*

- *Part 1: Key management framework*
- *Part 2: Mechanisms using symmetric techniques*
- *Part 3: Mechanisms using asymmetric techniques*

Further parts may follow.

Annexes A, B and C of this part of ISO/IEC 11770 are for information only.

ISO/IEC Copyright Office • Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Information technology — Security techniques — Key management —

Part 2:
Mechanisms using symmetric techniques

1 Scope

The purpose of key management is to provide procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic algorithms according to the security policy in force. This part of ISO/IEC 11770 defines key establishment mechanisms using symmetric cryptographic techniques.

Key establishment mechanisms using symmetric cryptographic techniques can be derived from entity authentication mechanisms of ISO/IEC 9798-2 and ISO/IEC 9798-4 by specifying the use of text fields available in those mechanisms. Other key establishment mechanisms exist for specific environments; see for example ISO 8732. Besides key establishment, goals of such a mechanism may include unilateral or mutual authentication of the communicating entities. Further goals may be the verification of the integrity of the established key, or key confirmation.

This part of ISO/IEC 11770 addresses three environments for the establishment of keys: Point-to-Point, Key Distribution Centre (KDC) and Key Translation Centre (KTC). This part of ISO/IEC 11770 describes the required content of messages which carry keying material or are necessary to set up the conditions under which the keying material can be established. The document does not indicate other information which may be contained in the messages or specify other messages such as error messages. The explicit format of messages is not within the scope of this part of ISO/IEC 11770.

This part of ISO/IEC 11770 does not explicitly address the issue of interdomain key management. This part of ISO/IEC 11770 also does not define the implementation of key management mechanisms; there may be different products that comply with this part of ISO/IEC 11770 and yet are not compatible.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 11770. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 11770 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498-2: 1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

ISO/IEC 9798-2: 1994, *Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms.*

ISO/IEC 9798-4: 1995, *Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function.*

ISO/IEC 11770-1: - [1], *Information technology - Security techniques - Key management - Part 1: Key management framework.*

3 Definitions and Notation

3.1 Definitions

For the purposes of this part of ISO/IEC 11770 the definitions given in ISO/IEC 11770-1 apply. In addition, this part of ISO/IEC 11770 makes use of the following terms:

3.1.1 **distinguishing identifier:** Information which unambiguously distinguishes an entity.

[1] To be published.

3.1.2 **entity authentication:** The corroboration that an entity is the one claimed.

3.1.3 **key confirmation:** The assurance for one entity that another identified entity is in possession of the correct key.

3.1.4 **key control:** The ability to choose the key, or the parameters used in the key computation.

3.1.5 **key generating function:** A function which takes as input a number of parameters, at least one of which shall be secret, and which gives as output keys appropriate for the intended algorithm and application. The function shall have the property that it shall be computationally infeasible to deduce the output without prior knowledge of the secret input.

3.1.6 **point-to-point key establishment:** The direct establishment of keys between entities, without involving a third party.

3.1.7 **random number:** A time variant parameter whose value is unpredictable.

3.1.8 **redundancy:** Any information that is known and can be checked.

3.1.9 **sequence number:** A time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period.

3.1.10 **time variant parameter:** A data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp.

3.2 Notation

Throughout this part of ISO/IEC 11770 the following notation is used:

X is the distinguishing identifier of entity X.

KDC denotes a Key Distribution Centre.

KTC denotes a Key Translation Centre.

T is the distinguishing identifier of the Key Distribution Centre or the Key Translation Centre.

F denotes keying material.

K_{XY} is a secret key associated with the entities X and Y.

R is a random number.

R_X is a random number issued by entity X.

T/N is a time stamp or a sequence number.

T_X/N_X is a time stamp or a sequence number issued by entity X.

TVP is a time variant parameter.

TVP_X is a time variant parameter issued by entity X.

eK(Z) is the result of the encipherment of data Z with a symmetric algorithm using the key K.

dK(Z) is the result of the decipherment of data Z with a symmetric algorithm using the key K.

vK(Z) is the result of a cryptographic check function computed on data Z using the key K. vK(Z) is also called message authentication code (MAC) and may be denoted as macK(Z).

f denotes a key generating function.

X || Y is the result of the concatenation of data items X and Y in that order.

The fields *Text1*, *Text2*, ... specified in the mechanisms may contain optional data for use in applications outside the scope of this part of ISO/IEC 11770 (they may be empty). Their relationship and contents depend upon the specific application. One such possible application is message authentication (see annex B for an example).

Likewise, optional plaintext text fields may be prepended or appended to any of the messages. They have no security implications and are not explicitly included in the mechanisms specified in this part of ISO/IEC 11770.

Data items that are optional in the mechanisms are shown in *italics*.

4 Requirements

The key establishment mechanisms specified in this part of ISO/IEC 11770 make use of symmetric cryptographic techniques, more specifically symmetric encipherment algorithms and/or key generating functions. The cryptographic algorithms and the key life-time shall be chosen such that it is computationally infeasible for a key to be deduced during its life-time. If the following additional requirements are not met, the key establishment process may be compromised or it cannot be implemented.

For those mechanisms making use of a symmetric encipherment algorithm, either assumption a) or assumption b) is required.

a) The encipherment algorithm, its mode of operation and the redundancy in the plaintext shall provide the recipient with the means to detect forged or manipulated data.

b) The integrity of the enciphered data shall be ensured by a data integrity mechanism. If a hash-function is used for this purpose the hash-code shall either be appended to the data before encipherment or be placed in a plaintext text field.

NOTES

1 - Modes of operation for block cipher algorithms are standardized in ISO/IEC 10116.

2 - A data integrity mechanism is standardized in ISO/IEC 9797. Hash-functions are standardized in ISO/IEC 10118.

3 - When a KDC or KTC is involved, assumptions a) and b) are not always equivalent in terms of the ability to detect unambiguously on which link an active attack is being performed. See Annex B for examples.

In each exchange specified in the mechanisms of clauses 5, 6 and 7, the recipient of a message shall know the claimed identity of the originator. If this is not the case from the context in which the mechanism is being used then this could, e.g., be achieved by the inclusion of identifiers in additional plaintext text fields of certain of the messages.

Keying material may be established using either secure or insecure communication channels. When using only symmetric cryptographic techniques, at least the first key shall be exchanged between two entities using a secure channel in order to allow secure communications.

The key establishment mechanisms in this part of ISO/IEC 11770 require the use of time variant parameters such as time stamps, sequence numbers, or random numbers. In this context the use of the term random number also includes unpredictable pseudo-random numbers. The properties of these parameters, in particular that they are non-repeating, are important for the security of these mechanisms. For additional information on time variant parameters see Annex B of ISO/IEC 9798-2.

5 Point-to-Point Key Establishment

The basic mechanism of every key establishment scheme is point-to-point key establishment which requires that the entities already share a key so that further keys may be established directly between the entities.

For the implementation of the mechanisms specified in this clause it is assumed that

- A key K_{AB} is shared by the entities A and B.
- At least one of A or B is able to generate, acquire or contribute to a secret key K as described in the individual mechanism.
- Security requirements are concerned with the confidentiality of K, and modification and replay detection.

5.1 Key Establishment Mechanism 1

In key establishment mechanism 1 the key K is derived from a time variant parameter TVP, e.g., a random number R, a time stamp T, or a sequence number N, using a key generating function. Key establishment mechanism 1 provides no authentication of the key K established by the mechanism. The mechanism requires that A is able to generate a TVP.

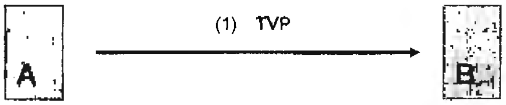


Figure 1 - Mechanism 1

Steps:

(1) A generates a random number R, a time stamp T, or a sequence number N and transfers it to B.

(1a) Both A and B then derive the key K by using a key generating function f with inputs the shared secret key K_{AB} and the time variant parameter TVP:

$$K = f(K_{AB}, TVP).$$

See Annex B for examples of possible key generating functions.

NOTE - To also provide authentication, key establishment mechanism 1 may be combined with an authentication mechanism as specified in 9798-2 or 9798-4. See annex B for an example.

5.2 Key Establishment Mechanism 2

In key establishment mechanism 2 the key K is supplied by entity A. The mechanism provides no authentication of the key K established by the mechanism nor does it provide entity authentication.

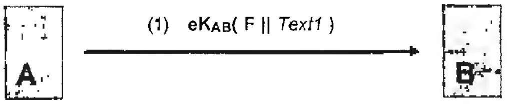


Figure 2 - Mechanism 2

Steps:

(1) A sends B the keying material F (key K and optional data) enciphered with K_{AB}.

(1a) On receipt of the message, B deciphers the enciphered part and thus obtains the key K.

5.3 Key Establishment Mechanism 3

Key establishment mechanism 3 is derived from the one pass entity authentication mechanism of ISO/IEC 9798-2, clause 5.1.1. In this mechanism the key K is supplied by entity A. Key establishment mechanism 3 provides unilateral authentication, i.e., entity A is authenticated by the mechanism. Uniqueness/timeliness is controlled by time stamps or sequence numbers. The mechanism requires that both A and B are able to maintain mechanisms for generating or verifying the validity of time stamps T or sequence numbers N.

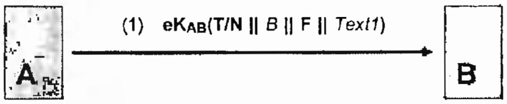


Figure 3 - Mechanism 3

Steps:

(1) A sends B a time stamp or sequence number T/N, the distinguishing identifier B, and the keying material F (key K and optional data). The inclusion of the distinguishing identifier B is optional. The data fields are enciphered with K_{AB}.

(1a) On receipt of the message, B deciphers the enciphered part, checks the correctness of its distinguishing identifier, if present, checks the time stamp or sequence number, and obtains the key K.

NOTE - Distinguishing identifier B is included in step (1) to prevent a substitution attack, i.e., the re-use of this message by an adversary masquerading as B (see Annex A). In environments where such attacks cannot occur, the identifier may be omitted.

5.4 Key Establishment Mechanism 4

Key establishment mechanism 4 is derived from the two pass unilateral entity authentication mechanism of ISO/IEC 9798-2, clause 5.1.2. In this mechanism the key K is supplied by entity A. Key establishment mechanism 4 provides unilateral authentication, i.e., entity A is authenticated by the mechanism. Uniqueness/timeliness is controlled by a random number R_B. The mechanism requires that B is able to generate random numbers.

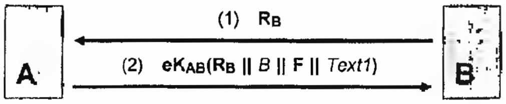


Figure 4 - Mechanism 4

Steps:

(1) B sends A a random number R_B.

(2) A sends B the received number R_B, the distinguishing identifier B, and the keying material F (key K and optional data). The inclusion of the distinguishing identifier B is optional. The data fields are enciphered with K_{AB}.

(2a) On receipt of message (2), B deciphers the enciphered part, checks the correctness of its distinguishing identifier, if present, checks that the random number R_B, sent to A in step (1), was used in constructing message (2), and obtains the key K.

NOTE - Distinguishing identifier B is included in step (2) to prevent a substitution attack, i.e., the re-use of this message by an adversary masquerading as B (see Annex A). In environments where such attacks cannot occur, the identifier may be omitted.

5.5 Key Establishment Mechanism 5

Key establishment mechanism 5 is derived from the two pass mutual authentication mechanism of ISO/IEC 9798-2, clause 5.2.1. This mechanism enables both A and B to contribute part of the established key K. Key establishment mechanism 5 provides mutual authentication, i.e., both communicating entities are authenticated by the mechanism. Uniqueness/timeliness is controlled by time stamps or sequence numbers. The mechanism requires that both A and B arc able to maintain mechanisms for generating and verifying the validity of time stamps T or sequence numbers N.

Steps:

(1) A sends B a time stamp or sequence number T_A/N_A, the distinguishing identifier B, and the keying material F_A. The inclusion of the

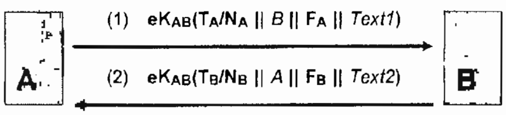

A
B
(1) $eK_{AB}(T_A/N_A \,||\, B \,||\, F_A \,||\, Text1)$
(2) $eK_{AB}(T_B/N_B \,||\, A \,||\, F_B \,||\, Text2)$

Figure 5 - Mechanism 5

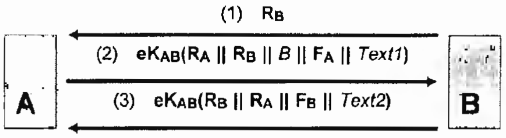

A
B
(1) R_B
(2) $eK_{AB}(R_A \,||\, R_B \,||\, B \,||\, F_A \,||\, Text1)$
(3) $eK_{AB}(R_B \,||\, R_A \,||\, F_B \,||\, Text2)$

Figure 6 - Mechanism 6

distinguishing identifier B is optional. The data fields are enciphered with K_{AB}.

(1a) On receipt of message (1), B deciphers the enciphered part, checks the correctness of its distinguishing identifier, if present, and checks the time stamp or sequence number.

(2) B sends A a time stamp or sequence number T_B/N_B, the distinguishing identifier A, and the keying material F_B. The inclusion of the distinguishing identifier A is optional. The data fields are enciphered with K_{AB}.

(2a) On receipt of message (2), A deciphers the enciphered part, checks the correctness of its distinguishing identifier, if present, and checks the time stamp or sequence number.

(2b) Both A and B derive the key K by using a key generating function f with inputs the secret keying material fields F_A and F_B:

$$K = f(F_A,F_B).$$

See Annex B for examples of possible key generating functions.

NOTES

1 - In key establishment mechanism 5, either of the two keying material fields F_A or F_B may be empty, but not both.

2 - Distinguishing identifier B is included in step (1) to prevent the re-use of this message by an adversary masquerading as B. For similar reasons, distinguishing identifier A is present in step (2). In environments where such attacks cannot occur, one or both of the identifiers may be omitted.

5.6 Key Establishment Mechanism 6

Key establishment mechanism 6 is derived from the three pass authentication mechanism of ISO/IEC 9798-2, clause 5.2.2. This mechanism enables both A and B to contribute part of the established key K. Key establishment mechanism 6 provides mutual authentication, i.e., both communicating entities are authenticated by the mechanism. Uniqueness/timeliness is controlled by random numbers. The mechanism requires that both A and B are able to generate random numbers.

Steps:

(1) B sends A a random number R_B.

(2) A sends B a random number R_A, the received number R_B, the distinguishing identifier B, and the keying material F_A. The inclusion of the distinguishing identifier B is optional. The data fields are enciphered with K_{AB}.

(2a) On receipt of message (2), B deciphers the enciphered part, checks the correctness of its distinguishing identifier, if present, and checks that the random number R_B, sent to A in step (1), was used in constructing message (2).

(3) B sends A the random numbers R_B and R_A, and the keying material F_B. The data fields are enciphered with K_{AB}.

(3a) On receipt of message (3), A deciphers the enciphered part and checks that the random number R_A, sent to B in step (2), was used in constructing message (3).

(3b) Both A and B derive the key K by using a key generating function f with inputs the secret keying material fields F_A and F_B:

$$K = f(F_A,F_B).$$

See Annex B for examples of possible key generating functions.

NOTES

1 - In key establishment mechanism 6, either of the two keying material fields F_A or F_B may be empty, but not both.

2 - Distinguishing identifier B is included in step (2) to prevent reflection attacks. In environments where such attacks cannot occur, the identifier may be omitted.

3 - A variant of key establishment mechanism 6 can be constructed from two parallel instances of mechanism 4, one started by entity A and the other by entity B.

6 Key Distribution Centre

The purpose of a Key Distribution Centre (KDC) is to generate or acquire and distribute keys to entities that each share a key with the KDC.

In this clause, four key establishment mechanisms are specified. In the first three mechanisms one of the two entities requests a key K from the KDC for later distribution to the other entity. The KDC generates or acquires the key K and sends a message to the requesting entity protected by a key shared with this entity. This message contains a second message protected by a key shared between the KDC and the second entity, which then can be sent by the requesting entity to the ultimate recipient. For the last mechanism the KDC generates or acquires the key K and sends it directly to each communicating entity. The messages are protected using the keys which the KDC shares with the corresponding entities. If required, authentication of the requesting entity by the KDC may be ensured by the inclusion of a MAC in a plaintext text field of the requesting message.

For all these mechanisms, only the KDC has to have the ability to generate or otherwise acquire keys. Following the distribution of a key by the KDC, the two entities may operate in a point-to-point mode.

For the implementation of the mechanisms specified in this clause it is assumed that

- There is a trusted third party T, the Key Distribution Centre, with which A and B share secret keys, K_{AT} and K_{BT} respectively. The KDC shall be able to generate or otherwise acquire a key K.
- The KDC is on-line with the entity requesting a key.
- Security requirements are concerned with the confidentiality of K, modification and replay detection, and the detection of substitution attacks.

6.1 Key Establishment Mechanism 7

In key establishment mechanism 7 the key K is supplied by the Key Distribution Centre. The mechanism provides no authentication of the key K established by the mechanism.

Steps:

(1) A requests keying material from the KDC by sending a message to the KDC that contains the distinguishing identifier of the recipient B.

(2) The KDC sends a protected message to A that contains the keying material F (key K and optional data). This message consists of 2 main parts:

(a) eK_{AT}(F || B || *Text1*)

(b) eK_{BT}(F || A || *Text2*)

(2a) On receipt of message (2), A deciphers part (a), checks the correctness of the distinguishing identifier and obtains the key K.

(3) A forwards part (b) of message (2) to B.

(3a) On receipt of message (3), B deciphers the enciphered part, checks the correctness of the distinguishing identifier and also obtains the key K.

6.2 Key Establishment Mechanism 8

Key establishment mechanism 8 is derived from the four pass authentication mechanism of ISO/IEC 9798-2, clause 6.1. In this mechanism the key K is supplied by the Key Distribution Centre. Key establishment mechanism 8 optionally provides mutual authentication, i.e., both communicating entities can be authenticated by the mechanism. Uniqueness/timeliness is controlled by time stamps or sequence numbers. The mechanism requires that A, B, and the KDC are able to maintain mechanisms for generating and verifying the validity of time stamps T or sequence numbers N.

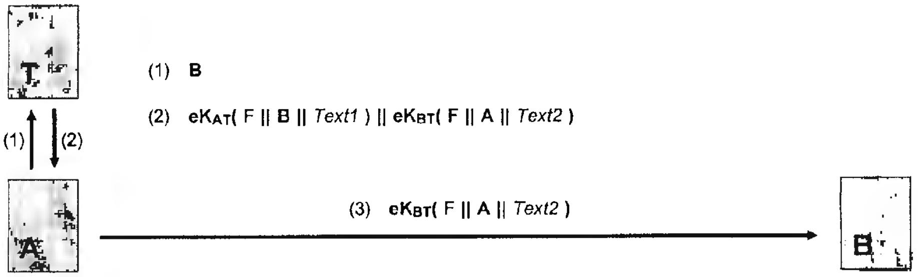

T
(1) B
(2) eKAT(F || B || Text1) || eKBT(F || A || Text2)
(1)
(2)
A
(3) eKBT(F || A || Text2)
B

Figure 7 - Mechanism 7

Steps:

(1) A requests keying material from the KDC by sending a message to the KDC that contains a time variant parameter TVP_A (a random number, time stamp, or sequence number) and the distinguishing identifier of the recipient B.

(2) The KDC sends a protected message to A that contains the keying material F (key K and optional data). This message consists of 2 main parts:

(a) $eK_{AT}(TVP_A \,||\, F \,||\, B \,||\, \mathit{Text1})$

(b) $eK_{BT}(T_T/N_T \,||\, F \,||\, A \,||\, \mathit{Text2})$

(2a) On receipt of message (2), A deciphers part (a), checks that the time variant parameter TVP_A, sent to the KDC in step (1), was used in constructing message (2), checks the correctness of the distinguishing identifier, and obtains the key K.

(3) A forwards part (b) of message (2) to B. Message (3) optionally contains a data field $eK(T_A/N_A \,||\, B \,||\, \mathit{Text3})$ which enables B to check the integrity of the key K retrieved from F.

(3a) On receipt of message (3), B deciphers the first part, checks the correctness of the time stamp or sequence number, and obtains the key K. The distinguishing identifier indicates to B that the key was requested by A.

(3b) B deciphers the second part of message (3), if present, and checks the correctness of the time variant parameter and of its distinguishing identifier.

Optional:

The following can be omitted if no or only unilateral entity authentication is required.

(4) B returns $eK(T_B/N_B \,||\, A \,||\, \mathit{Text4})$ to A thereby acknowledging that it shares the key K.

(4a) On receipt of message (4), A deciphers it and checks the correctness of the time variant parameter and of the distinguishing identifier.

NOTES

1 - The encipherment algorithm e used in the optional key confirmation process may differ from the encipherment algorithm (also denoted by e) used for key distribution.

2 - To achieve mutual authentication and conformance with the four pass authentication mechanism specified in ISO/IEC 9798-2 the options in steps (3) and (3b) and optional steps (4) and (4a) need to be included.

6.3 Key Establishment Mechanism 9

Key establishment mechanism 9 is derived from the five pass authentication mechanism of ISO/IEC 9798-2, clause 6.2. In this mechanism the key K is supplied by the Key Distribution Centre. Key establishment mechanism 9 optionally provides mutual authentication, i.e., both communicating entities can be authenticated by the mechanism. Uniqueness/timeliness is controlled by random numbers. The mechanism requires that A, B and the KDC are able to generate random numbers.

Steps:

(1) B initiates the mechanism by sending a random number R_B to A.

(2) A requests keying material from the KDC by sending a message to the KDC that contains a random number R_A, the random number R_B, and the distinguishing identifier of B.

(3) The KDC sends a protected message to A that contains the keying material F (key K and optional data). This message consists of 2 main parts:

(a) $eK_{AT}(R_A \,||\, F \,||\, B \,||\, \mathit{Text1})$

(b) $eK_{BT}(R_B \,||\, F \,||\, A \,||\, \mathit{Text2})$

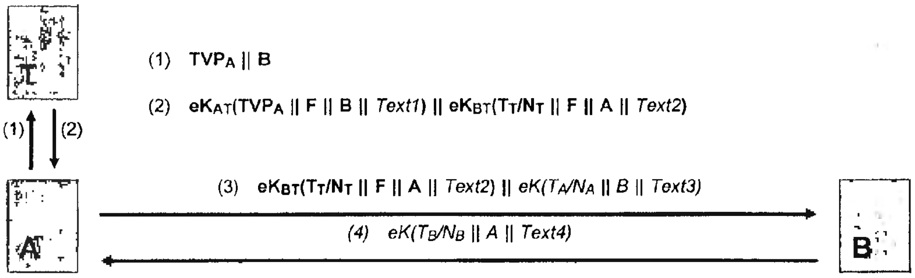

KDC
(1) TVPA || B
(2) eKAT(TVPA || F || B || Text1) || eKBT(TT/NT || F || A || Text2)
(1)
(2)
A
(3) eKBT(TT/NT || F || A || Text2) || eK(TA/NA || B || Text3)
(4) eK(TB/NB || A || Text4)
B

Figure 8 - Mechanism 8

(3a) On receipt of message (3), A deciphers part (a), checks that the random number R_A, sent to the KDC in step (2), was used in constructing message (3), checks the correctness of the distinguishing identifier, and retrieves the key K.

(4) A forwards part (b) of message (3) to B. Message (4) optionally contains a data field $eK(R'_A \| R_B \| \textit{Text3})$ which incorporates random numbers R_B and R'_A and enables B to check the integrity of the key K retrieved from F.

(4a) On receipt of message (4), B deciphers the first part, checks that the random number R_B, sent to A in step (1), was used in constructing message (4), and obtains the key K. The distinguishing identifier indicates to B that the key was requested by A.

(4b) B deciphers the second part of message (4), if present, and checks that the random number R_B, sent to A in step (1), was used in constructing the second part of message (4).

Optional:

The following can be omitted if no or only unilateral entity authentication is required.

(5) B returns $eK(R_B \| R'_A \| \textit{Text4})$ to A thereby acknowledging that it also shares the key K. Step (5) requires the option described in step (4).

(5a) On receipt of message (5), A deciphers it and checks that the random number R'_A, sent to B in step (4), was used in constructing message (5).

NOTES

1 - The encipherment algorithm e used in the optional key confirmation process may differ from the encipherment algorithm (also denoted hy e) used for key distribution.

2 - To achieve mutual authentication and conformance with the five pass authentication mechanism specified in ISO/IEC 9798-2 the options in steps (4) and (4b) and optional steps (5) and (5a) need to be included.

6.4 Key Establishment Mechanism 10

In key establishment mechanism 10 the KDC distributes the keying material directly to both entities. The mechanism provides mutual authentication between A and the KDC and unilateral authentication from the KDC to B. Uniqueness/timeliness is controlled by time stamps or sequence numbers. The mechanism requires that A, B, and the KDC are able to maintain mechanisms for generating or verifying the validity of time stamps T or sequence numbers N.

Steps:

(1) A requests keying material from the KDC by sending a message to the KDC that contains a time stamp or sequence number T_A/N_A, and the distinguishing identifier of the recipient B. The data fields are enciphered with K_{AT}.

(1a) On receipt of message (1), the KDC deciphers it and checks the correctness of the time stamp or sequence number.

(2) The KDC returns a message to A that contains a time time stamp or sequence number T_T/N_T, the distinguishing identifier of B, and the keying material F. The data fields are enciphered with K_{AT}.

(2a) On receipt of message (2), A deciphers it, checks the correctness of the time stamp or sequence number, and obtains the key K.

(3) The KDC sends a message to B that contains a time stamp or sequence number T'_T/N'_T, the distinguishing identifier of A, and the keying material F. The data fields are enciphered with K_{BT}.

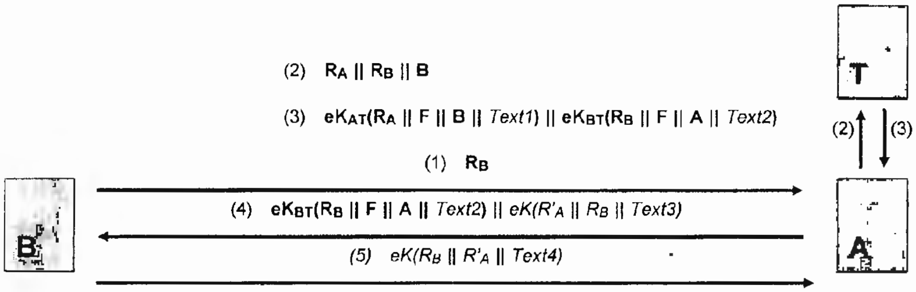

(2) $R_A \| R_B \| B$
(3) $eK_{AT}(R_A \| F \| B \| \textit{Text1}) \| eK_{BT}(R_B \| F \| A \| \textit{Text2})$
T
(2)
(3)
(1) R_B
(4) $eK_{BT}(R_B \| F \| A \| \textit{Text2}) \| eK(R'_A \| R_B \| \textit{Text3})$
B
A
(5) $eK(R_B \| R'_A \| \textit{Text4})$

Figure 9 - Mechanism 9

(3a) On receipt of message (3), B deciphers it, checks the correctness of the time stamp or sequence number, and obtains the key K. The distinguishing identifier of A indicates to B that the key was requested by A.

NOTES

1 - The order of steps 2 and 3 is optional.

2 - There is no authentication between A and B. After key establishment, entity authentication can be achieved using one of the mechanisms of ISO/IEC 9798-2 or ISO/IEC 9798-4.

7 Key Translation Centre

The purpose of a Key Translation Centre is to translate keys between entities that each share a key with the KTC. One of the entities (the originator) sends a key K to the KTC enciphered with a key shared between the originator and the KTC. The KTC deciphers the key K and re-enciphers it with a key shared with the second entity (the ultimate recipient); this process produces the translated key. The KTC then either

(a) sends the translated key back to the originator who then forwards it to the ultimate recipient, or

(b) forwards the translated key to the ultimate recipient directly.

In an environment where a KTC is used the originator shall have the ability to generate or otherwise acquire keys.

For the implementation of the mechanisms specified in this clause it is assumed that

- There is a trusted third party T, the Key Translation Centre, with which A and B share secret keys, K_{AT} and K_{BT} respectively.
- The KTC is on-line with at least one of the entities, usually the originator.
- The originator is able to generate or otherwise acquire a secret key K.
- Security requirements are concerned with the confidentiality of K, modification and replay detection, and the detection of substitution attacks.

7.1 Key Establishment Mechanism 11

In key establishment mechanism 11 the key K is supplied by entity A. The mechanism provides no authentication of the key K established by the mechanism.

Steps:

(1) A requests a key translation by sending a message to the KTC that is enciphered with K_{AT} and contains the distinguishing identifier of the recipient B, and the keying material F (key K and optional data).

(1a) On receipt of message (1), the KTC deciphers F, adds the distinguishing identifier A and re-enciphers both with K_{BT}.

(2) The KTC returns the re-enciphered keying material to A.

(3) A forwards the protected part of message (2) to B.

(3a) On receipt of message (3), B deciphers the enciphered part and thus obtains the key K. The distinguishing identifier of A indicates to B that the key was requested by A.

7.2 Key Establishment Mechanism 12

Key establishment mechanism 12 is derived from, but is not fully compatible with, the four pass authentication mechanism of ISO/IEC 9798-2:1994, clause 6.1. In this mechanism the key K is supplied by entity A.

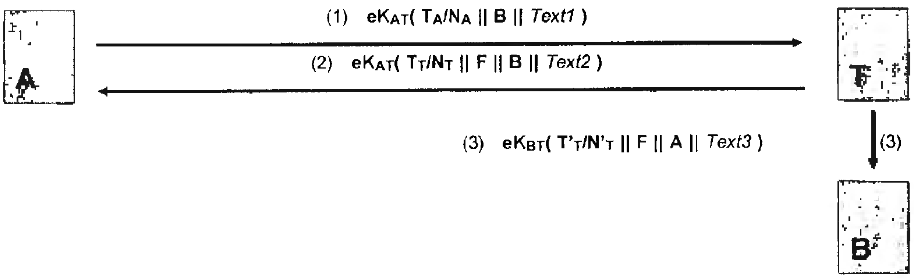

A
(1) $eK_{AT}(\ T_A/N_A \ || \ B \ || \ \mathit{Text1}\ )$
(2) $eK_{AT}(\ T_T/N_T \ || \ F \ || \ B \ || \ \mathit{Text2}\ )$
T
(3) $eK_{BT}(\ T'_T/N'_T \ || \ F \ || \ A \ || \ \mathit{Text3}\ )$
(3)
B

Figure 10 - Mechanism 10

Uniqueness/timeliness is controlled by time stamps or sequence numbers.

Key establishment mechanism 12 optionally provides mutual authentication, i.e., both communicating entities can be authenticated by the mechanism. The mechanism requires that A, B and the KTC are able to maintain mechanisms for generating and verifying the validity of time stamps T or sequence numbers N.

Steps:

(1) A requests a key translation by sending a message to the KTC that consists of a time variant parameter TVP_A (a random number, time stamp or sequence number), the distinguishing identifier of the recipient B, and the keying material F (key K and optional data). The data fields are enciphered with K_{AT}.

(1a) On receipt of message (1), the KTC deciphers the enciphered keying material F and re-enciphers it together with additional data fields.

(2) The KTC returns a message to A that consists of 2 main parts:

(a) $eK_{AT}(TVP_A \| B \| \mathit{Text2})$

(b) $eK_{BT}(T_T/N_T \| F \| A \| \mathit{Text3})$

(2a) On receipt of message (2), A deciphers the first part and checks the distinguishing identifier and that the time variant parameter TVP_A, sent to the KDC in step (1), was used in constructing message (2).

(3) A forwards part (b) of message (2) to B. Message (3) optionally contains a data field $eK(T_A/N_A \| B \| \mathit{Text4})$ which enables B to check the integrity of the key K retrieved from F.

(3a) On receipt of message (3), B deciphers the first part, checks the correctness of the time stamp or sequence number, and obtains the key K. The distinguishing identifier indicates to B that the key translation was requested by A.

(3b) B deciphers the second part of message (3), if present, and checks the correctness of the time variant parameter and of its distinguishing identifier.

Optional:

The following can be omitted if no or only unilateral entity authentication is required.

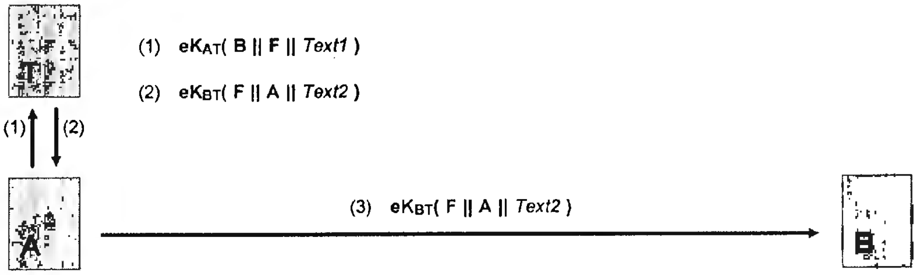

T
(1) eK_AT(B || F || Text1)
(2) eK_BT(F || A || Text2)
(1)
(2)
A
(3) eK_BT(F || A || Text2)
B

Figure 11 - Mechanism 11

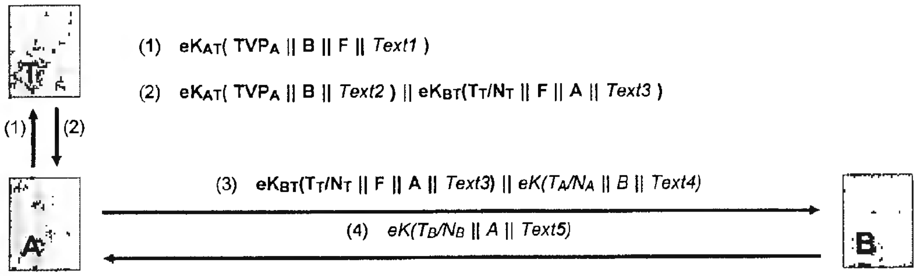

T
(1) eK_AT(TVP_A || B || F || Text1)
(2) eK_AT(TVP_A || B || Text2) || eK_BT(T_T/N_T || F || A || Text3)
(1)
(2)
A
(3) eK_BT(T_T/N_T || F || A || Text3) || eK(T_A/N_A || B || Text4)
(4) eK(T_B/N_B || A || Text5)
B

Figure 12 - Mechanism 12

(4) B returns $eK(T_B/N_B \,||\, A \,||\, Text5)$ to A thereby acknowledging that it shares the key K.

(4a) On receipt of message (4), A deciphers it and checks the correctness of the time variant parameter and of its distinguishing identifier.

NOTES

1 - The encipherment algorithm e used in the optional key confirmation process may differ from the encipherment algorithm (also denoted by e) used for key distribution.

2 - To achieve mutual authentication the options in steps (3) and (3b) and optional steps (4) and (4a) need to be included.

7.3 Key Establishment Mechanism 13

Key establishment mechanism 13 is derived from, but is not fully compatible with, the five pass authentication mechanism of ISO/IEC 9798-2:1994, clause 6.2. In this mechanism the key K is supplied by entity A. Key establishment mechanism 13 optionally provides mutual authentication, i.e., both communicating entities can be authenticated by the mechanism. Uniqueness/timeliness is controlled by random numbers. The mechanism requires that A, B and the KTC are able to generate random numbers.

Steps:

(1) B initiates the mechanism by sending a random number R_B to A.

(2) A requests a key translation by sending a message to the KTC that contains a random number R_A, the random number R_B, the distinguishing identifier of the originator B, and the keying material F (key K and optional data). The data fields are enciphered with K_{AT}.

(2a) On receipt of message (2), the KTC deciphers the enciphered keying material F and re-enciphers it together with additional data fields.

(3) The KTC returns a message to A that consists of 2 main parts:

(a) $eK_{AT}(R_A \,||\, B \,||\, Text2)$

(b) $eK_{BT}(R_B \,||\, F \,||\, A \,||\, Text3)$

(3a) On receipt of message (3), A deciphers part (a) and checks the distinguishing identifier and that the random number R_A, sent to the KTC in step (2), was used in constructing message (3).

(4) A forwards part (b) of message (3) to B. Message (4) optionally contains a data field $eK(R'_A \,||\, R_B \,||\, Text4)$ which enables B to check the integrity of the key K retrieved from F.

(4a) On receipt of message (4), B deciphers its first part and obtains the key K. If the random number R_B sent to A in step (1), was used in constructing the first part of message (4), the message indicates to B that it was sent by A as a reply to message (1).

(4b) If present, B deciphers the second part of message (4) and checks that the random number R_B sent to A in step (1), was also used in constructing the second part of message (4).

Optional:

The following can be omitted if no or only unilateral entity authentication is required.

(5) B returns $eK(R_B \,||\, R'_A \,||\, Text5)$ to A thereby acknowledging that it also shares the key K. Step (5) requires the option described in step (4).

(5a) On receipt of message (5), A checks that the random number R'_A sent to B in step (4), was used in constructing message (5).

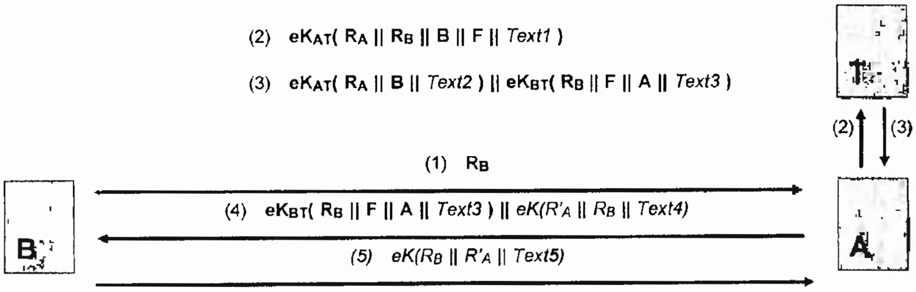

(2) eKAT(RA || RB || B || F || Text1)
(3) eKAT(RA || B || Text2) || eKBT(RB || F || A || Text3)
T
(2)
(3)
(1) RB
(4) eKBT(RB || F || A || Text3) || eK(R'A || RB || Text4)
(5) eK(RB || R'A || Text5)
B
A

Figure 13 - Mechanism 13

NOTES

1 - The encipherment algorithm e used in the optional key confirmation process may differ from the encipherment algorithm (also denoted by e) used for key distribution.

2 - To achieve mutual authentication the options in steps (4) and (4b) and optional steps (5) and (5a) need to be included.

Annex A
(informative)

Properties of Key Establishment Mechanisms

Table A.1 summarizes major properties of the key establishment mechanisms specified in this part of ISO/IEC 11770. Options are shown in parenthesis, e.g., mechanism 8 has an optional fourth pass to achieve mutual entity authentication.

Table A.1

Mechanism	1	2	3	4	5	6	7	8	9	10	11	12	13
Role of third party	-	-	-	-	-	-	KDC	KDC	KDC	KDC	KTC	KTC	KTC
Number of passes	1	1	1	2	2	3	3	3(4)	4(5)	3	3	3(4)	4(5)
Key control	entity A[1]	entity A	entity A	entity A	A/B	A/B	KDC	KDC	KDC	KDC	entity A	entity A	entity A
Key authentication[2]	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Replay detection[3]	no	no	T/N	R	T/N	R	no	T/N	R	T/N	no	T/N	R
Key confirmation[4]	no	no	no	no	no	no	no	opt.	opt.	no	no	opt.	opt.
Entity authentication[5]	no	no	A	A	A + B	A + B	no	opt.	opt.	no	no	opt.	opt.

NOTES

1 - In case of mechanism 1, the key K is not directly supplied by entity A but derived from a time variant parameter provided by A.

2 - Key authentication in this context refers to explicit key authentication and includes both key integrity and key origin authentication. All the mechanisms offer at least implicit key authentication, because only parties with knowledge of a specific secret key can recover the correct key.

3 - T/N denotes replay detection by using time stamps or sequence numbers while R denotes replay detection by using random numbers.

4 - Key confirmation can optionally be achieved for every mechanism using the technique specified in Annex B.

5 - Entity authentication in this context only refers to authentication between entities A and B. In case of mechanisms 8, 9, 12 and 13, unilateral or mutual authentication can optionally be achieved.

Distinguishing identifiers are included in the enciphered parts of messages of some of the mechanisms to protect against certain types of substitution attacks, i.e., the re-use of legitimate messages of A or B by a third party wishing to masquerade as one of A or B. More specifically, in some cases the inclusion of distinguishing identifiers is used to protect against reflection attacks, which are a specific form of substitution attack where a message sent by one entity (A say) is sent back to that entity by a masquerading third party, in order to convince A that it is communicating with a legitimate entity. In environments where reflection attacks cannot occur, and where the text accompanying the message description makes it clear that this is allowed, distinguishing identifiers may bc omitted. One particular case where reflection attacks cannot occur is when the authenticating entities A and B share two different secret keys (unidirectional keys) used separately for messages sent from A to B, and for messages sent from B to A.

Annex B
(informative)

Auxiliary Techniques

B.1 Data Integrity

In the key establishment mechanisms specified in this part of ISO/IEC 11770, the text fields may be used to ensure data integrity. If a hash-function is used for this purpose the hash-code shall either be appended to the data before encipherment or placed in a plaintext text field. If a message authentication code is used the MAC may be calculated with a key derived from the established key K. In all cases the recipient of K can check the integrity of the received message and of the retrieved key.

To ensure data integrity of a message

$$eK_{AB}(\ldots \| K \| Text1)$$

Text1 may be replaced by

$$Text1^* \| h(\ldots \| K \| Text1^*)$$

where h(X) denotes the hash-code of data X, or a plaintext text field

$$macK^*(eK_{AB}(\ldots \| K \| Text1))$$

may be appended where K* denotes a key derived from K.

When two concatenated enciphered data fields are sent back by a KDC or KTC (as in mechanisms 7, 8, 9, 12, 13) assumptions a) and b) of section 4 are not always equivalent. Assumption a) can only guarantee individually the integrity of each enciphered part while assumption b) can in addition guarantee the integrity of the message as a whole. Only in the second case it is possible to detect unambiguously on which link an active attack is being performed.

As an example, for a mechanism where

$$eK_{AT}(\ldots) \| eK_{BT}(\ldots)$$

is sent from T to A, in order to detect a modification of any part of the message on the link between T and A, a plaintext text field

$$macK_{AT}^*(eK_{AT}(\ldots) \| eK_{BT}(\ldots)) \| macK_{BT}^*(eK_{BT}(\ldots))$$

may be appended where K_{AT}^* and K_{BT}^* denote keys derived from K_{AT} and K_{BT}.

B.2 Key Calculation

Key calculation is a technique for obtaining a key from two or more data items, at least one of which is secret, using a key generating function f (which may be publicly known). Examples of such functions are as follows:

(a) The bitwise modulo 2 sum of two secret data items F_1 and F_2, i.e.

$$K = f(F_1, F_2) = F_1 \oplus F_2$$

(b) Applying a hash-function h, as defined in ISO/IEC 10118, to the concatenation of two data items F_1 and F_2, at least one of which is a shared secret, i.e.

$$K = f(F_1, F_2) = h(F_1 \| F_2).$$

In some situations it is desirable for a key generating function to be one-way, i.e. given knowledge of the output it shall be computationally infeasible to obtain any information regarding the secret input parameter(s). Note that example function (a) above is not one-way in this sense, since knowledge of the output K immediately yields useful information regarding the two secret input parameters F_1 and F_2. In key establishment mechanism 1 it is necessary for the key generating function to have the one-way property, so that if key K obtained using the mechanism is compromised, then the shared secret K_{AB} (which may be a 'long term' shared secret) is not compromised.

B.3 Key Offsetting

Key offsetting is a technique for obtaining additional keys from a single key. An example of how to derive a key K* from a given key K is to complement alternate blocks of four bits of K commencing with the first four bits.

B.4 Key Confirmation

Key confirmation is a technique for assuring one entity that another identified entity is in possession of the correct key. An example of how an entity X may acknowledge to entity Y that it shares the key K is to send

$$eK(TVP || Text)$$

to Y, where TVP denotes a time variant parameter known by entity Y.

B.5 Combination of Key Establishment and Authentication

To also provide authentication, key establishment mechanisms may be combined with an authentication mechanism as specified in 9798-2 or 9798-4. The example given below shows the result of the combination of key establishment mechanism 1 with the two pass unilateral authentication mechanism specified in ISO/IEC 9798-4, clause 5.1.2.

Steps:

(1) B generates a random number R_B and transfers it to A.

(1a) Both A and B derive the key K by applying a cryptographic check function v keyed with the shared key K_{AB} to the random number R_B:

$$K = vK_{AB}(R_B).$$

(2) A returns $v'K_{AB}(R_B || B)$ to B, a cryptographic check value of the received number R_B and the distinguishing identifier B.

(2a) On receipt of message (2), B checks that its distinguishing identifier and the random number R_B, sent to A in step (1), were used in constructing message (2).

Annex C
(informative)

Bibliography

[1] ISO 8732: 1988, *Banking - Key Management (wholesale).*

[2] ISO/IEC 9797: 1994, *Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.*

[3] ISO/IEC 9798-1: 1991, *Information technology - Security techniques - Entity authentication mechanisms - Part 1: General model.*

[4] ISO/IEC 10116: 1991, *Information technology - Modes of operation for an n-bit block cipher algorithm.*

[5] ISO/IEC 10118-1: 1994, *Information technology - Security techniques - Hash-functions - Part 1: General.*

[6] ISO/IEC 10118-2: 1994, *Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher algorithm.*

[7] ISO 11568-3: 1994, *Banking - Key management (retail) - Part 3: Key life cycle for symmetric ciphers.*

ICS 35.040

Descriptors: data processing, information interchange, data transmission, protection of information, security techniques, authentication, algorithms, key management.

Price based on 17 pages

INTERNATIONAL STANDARD

ISO/IEC 11770-3

First edition
1999-11-01

Information technology — Security techniques — Key management —

Part 3: Mechanisms using asymmetric techniques

Technologies de l'information — Techniques de sécurité — Gestion de clés —

Partie 3: Mécanismes utilisant des techniques asymétriques

Reference number
ISO/IEC 11770-3:1999(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 11770 may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 11770-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 11770 consists of the following parts, under the general title *Information technology — Security techniques — Key management*:

— *Part 1: Framework*

— *Part 2: Mechanisms using symmetric techniques*

— *Part 3: Mecanisms using asymmetruc techniques*

Further parts may follow.

Annexes A to E of this part of ISO/IEC 11770 are for information only.

Information technology — Security techniques — Key management —

Part 3: Mechanisms using asymmetric techniques

1. Scope

This part of ISO/IEC 11770 defines key management mechanisms based on asymmetric cryptographic techniques. It specifically addresses the use of asymmetric techniques to achieve the following goals:

1. Establish a shared secret key for a symmetric cryptographic technique between two entities *A* and *B* by key agreement. In a secret key agreement mechanism the secret key is the result of a data exchange between the two entities *A* and *B*. Neither of them can predetermine the value of the shared secret key.
2. Establish a shared secret key for a symmetric cryptographic technique between two entities *A* and *B* by key transport. In a secret key transport mechanism the secret key is chosen by one entity *A* and is transferred to another entity *B*, suitably protected by asymmetric techniques.
3. Make an entity's public key available to other entities by key transport. In a public key transport mechanism, the public key of an entity A must be transferred to other entities in an authenticated way, but not requiring secrecy.

Some of the mechanisms of this part of ISO/IEC 11770 are based on the corresponding authentication mechanisms in ISO/IEC 9798-3.

This part of ISO/IEC 11770 does not cover aspects of key management such as

- key lifecycle management,
- mechanisms to generate or validate asymmetric key pairs,
- mechanisms to store, archive, delete, destroy, etc. keys.

While this part of ISO/IEC 11770 does not explicitly cover the distribution of an entity's private key (of an asymmetric key pair) from a trusted third party to a requesting entity, the key transport mechanisms described can be used to achieve this.

This part of ISO/IEC 11770 does not cover the implementations of the transformations used in the key management mechanisms.

NOTE - To achieve authenticity of key management messages it is possible to make provisions for authenticity within the key establishment protocol or to use a public key signature system to sign the key exchange messages.

2. Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO 11770. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO 11770 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 7498-2:1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

ISO/IEC 9594-8:1995, *Information technology - Open Systems Interconnection – The Directory: Authentication framework.*

ISO/IEC 9798-3:1998, *Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques.*

ISO/IEC 10118-1:1994, *Information technology - Security techniques - Hash-functions - Part 1: General.*

ISO/IEC 10181-1:1996, *Information technology - Open Systems Interconnection - Security frameworks for open systems Overview.*

ISO/IEC 11770-1:1996, *Information technology - Security techniques - Key management - Part 1: Framework.*

3. Definitions

For the purposes of this part of ISO/IEC 11770, the following definitions apply.

3.1. asymmetric cryptographic technique: a cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation.

NOTE - A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques there are four elementary transformations: sign and verify for signature systems, encipher and decipher for encipherment systems. The signature and the decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformations are published. There exist asymmetric cryptosystems (e.g. RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one public transformation suffices for both verifying and encrypting messages. However, since this does not conform to the principle of key separation, throughout this part of ISO/IEC 11770 the four elementary transformations and the corresponding keys are kept separate.

3.2. asymmetric encipherment system: a system based on asymmetric cryptographic techniques whose public transformation is used for encipherment and whose private transformation is used for decipherment.

3.3. asymmetric key pair: a pair of related keys where the private key defines the private transformation and the public key defines the public transformation.

3.4. certification authority (CA): a center trusted to create and assign public key certificates. Optionally, the certification authority may create and assign keys to the entities.

3.5. cryptographic check function: a cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output. The computation of a correct check value without knowledge of the secret key shall be infeasible [ISO/IEC 9798-1:1997].

3.6. cryptographic check value: information which is derived by performing a cryptographic transformation on the data unit [ISO/IEC 9798-4:1995].

3.7. decipherment: the reversal of a corresponding encipherment [ISO/IEC 11770-1:1996].

3.8. digital signature: a data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient.

3.9. distinguishing identifier: information which unambiguously distinguishes an entity [ISO/IEC 11770-1:1996].

3.10. encipherment: the (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e. to hide the information content of the data [ISO/IEC 11770-1:1996].

3.11. entity authentication: the corroboration that an entity is the one claimed [ISO/IEC 9798-1:1997].

3.12. entity authentication of A to B: the assurance of the identity of entity A for entity B.

3.13. explicit key authentication from A to B: the assurance for entity B that A is the only other entity that is in possession of the correct key.

NOTE - implicit key authentication from A to B and key confirmation from A to B together imply explicit key authentication from A to B.

3.14. implicit key authentication from A to B: the assurance for entity B that A is the only other entity that can possibly be in possession of the correct key.

3.15. key: a sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature calculation, or signature verification) [ISO/IEC 11770-1:1996].

3.16. key agreement: the process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key.

3.17. key confirmation from A to B: the assurance for entity B that entity A is in possession of the correct key.

3.18. key control: the ability to choose the key or the parameters used in the key computation.

3.19. key establishment: the process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.

3.20. key token: key management message sent from one entity to another entity during the execution of a key management mechanism.

3.21. key transport: the process of transferring a key from one entity to another entity, suitably protected.

3.22. mutual entity authentication: entity authentication which provides both entities with assurance of each other's identity.

3.23. one-way function : a function with the property that it is easy to compute the output for a given input but it is computationally infeasible to find for a given output an input which maps to this output.

3.24. private key: that key of an entity's asymmetric key pair which can only be used by that entity.

NOTE - In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation.

3.25. public key that key of an entity's asymmetric key pair which can be made public

NOTE - In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

3.26. public key certificate the public key information of an entity signed by the certification authority and thereby rendered unforgeable.

3.27. public key information: information containing at least the entity's distinguishing identifier and public key. The public key information is limited to data regarding one entity, and one public key for this entity. There may be other static information regarding the certification authority, the entity, the public key, restrictions on key usage, the validity period, or the involved algorithms, included in the public key information.

3.28. secret key: a key used with symmetric cryptographic techniques by a specified set of entities.

3.29. sequence number: a time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period [ISO/IEC 11770-1:1996].

3.30. signature system: a system based on asymmetric cryptographic techniques whose private transformation is used for signing and whose public transformation is used for verification.

3.31. time stamp: a data item which denotes a point in time with respect to a common time reference.

3.32. time stamping authority: a trusted third party trusted to provide evidence which includes the time when the secure time stamp is generated [ISO/IEC 13888-1:1997].

3.33. time variant parameter: a data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp.

3.34. **trusted third party**: a security authority, or its agent, trusted by other entities with respect to security related activities [ISO/IEC 10181-1:1996].

4. Symbols and abbreviations

Thc following symbols and abbreviations are used in this part of ISO/IEC 11770.

A,*B*	distinguishing identifiers of entities.
BE	enciphered data block
BS	signed data block
CA	certification authority.
$Cert_A$	entity *A*'s public key certificate
D_A	entity *A*'s private decipherment transformation.
d_A	entity *A*'s private decipherment key.
E_A	entity *A*'s public encipherment transformation.
e_A	entity *A*'s public encipherment key.
F(h,g)	the key agreement function.
f	cryptographic check function
$f_K(Z)$	cryptographic check value which is the result of applying the cryptographic check function *f* using as input a secret key *K* and an arbitrary data string *Z*.
g	the common element shared publicly by all the entities that use the key agreement function *F*.
h_A	entity *A*'s private key agreement key.
hash	hash-function
H	set of elements
G	set of elements
K	a secret key for a symmetric cryptosystem.
K_{AB}	a secret key shared between entities *A* and *B*.

NOTE - In practical implementations the shared secret key may be subject to further processing before it can be used for a symmetric cryptosystem.

KT	key token.
KT_{Ai}	the key token sent by entity *A* after processing phase i.
p_A	cntity *A*'s public key agreement key.
PKI_A	cntity *A*'s public key information
r	a random number generated in the course of a mechanism.
r_A	a random number issued by entity *A* in a key agreement mechanism.
S_A	entity *A*'s private signature transformation.
s_A	entity *A*'s private signature key.
Texti	an optional data field whose use is beyond the scope of this part of ISO/IEC 11770.
TVP	time-variant parameter, such as a random number, a time stamp, or a sequence number.
V_A	entity *A*'s public verification transformation.
v_A	entity *A*'s public verification key.
w	one-way function
Σ	the digital signature
$\|\|$	concatenation of two data elements.

NOTES

1. No assumption is made on the nature of the signature transformation. In the case of a signature system with message recovery, $S_A(m)$ denotes the signature Σ itself. In the case of a signature system with appendix, $S_A(m)$ denotes the message *m* together with signature Σ.

2. The keys of an asymmetric cryptosystem are denoted by a lower case letter (indicating the function of that key) indexed with the identifier of its owner, e.g. the public verification key of entity *A* is denoted by v_A. The corresponding transformations are denoted by upper case letters indexed with the identifier of their owner, e.g. the public verification transformation of cntity *A* is denoted by V_A.

5. Requirements

It is assumed that the entities are aware of each other's claimed identities. This may be achieved by the inclusion of identifiers in information exchanged between the two entities, or it may be apparent from the context of the use of the mechanism. Verifying the identity means to check that a received identifier field agrees with some known (trusted) value or prior expectation.

If a public key is registered with an entity then that entity shall make sure that the entity who registers the key is in possession of the corresponding private key (see Part 1 for registration of key).

6. Secret key agreement

Key agreement is the process of establishing a shared secret key between two entities A and B in such a way that neither of them can predetermine the value of the shared secret key. Key agreement mechanisms may provide for implicit key authentication; in the context of key establishment, implicit key authentication means that after the execution of the mechanism only an identified entity can be in possession of the correct shared secret key.

The key agreement between two entities A and B takes place in a context shared by the two entities. The context consists of the following objects: a set G, a set H and a function F. The function F shall satisfy the following requirements:

1. F operates on two inputs, one element h from H and one element g from G, and produces a result y in G, $y = F(h,g)$.
2. F satisfies the commutativity condition $F(h_A,F(h_B,g)) = F(h_B,F(h_A,g))$.
3. It is computationally intractable to find $F(h_1,F(h_2,g))$ from $F(h_1,g)$, $F(h_2,g)$ and g. This implies that $F(\cdot,g)$ is a one-way function.
4. The entities A and B share a common element g in G which may be publicly known.
5. The entities acting on this setting can efficicntly compute function values $F(h,g)$ and can efficiently generate random elements in H.

Depending on the particular key agreement mechanism further conditions may be imposed.

NOTES

1. An example of a possible function F is given in Annex B.
2. In practical implementations of the key agreement mechanisms the shared secret key may be subject to further processing. A derived shared secret key may be computed (1) by extracting bits from the shared secret key K_{AB} directly or (2) by passing the shared secret K_{AB} and optionally other nonsecret data through a one-way function and extracting bits from the output.
3. It will in general be necessary to check the received function values $F(h,g)$ for weak values. If such values are encountered, the protocol shall be aborted. An example known as Diffie-Hellman key agreement is given in clause B.5.

6.1 Key agreement mechanism 1

This key agreement mechanism non-interactively establishes a shared secret key between entities A and B with mutual implicit key authentication. The following requirements shall be satisfied:

1. Each entity X has a private key agreement key h_X in H and a public key agreement key $p_X = F(h_X,g)$.
2. Each entity has access to an authenticated copy of the public key agreement key of the other entity. This may be achieved using the mechanisms of clause 8.

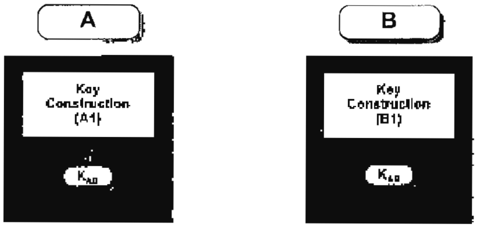


Figure 1 - Key Agreement Mechanism 1

Key Construction (A1) A computes, using its own private key agreement key h_A and B's public key agreement key p_B, the shared secret key as

$$K_{AB} = F(h_A, p_B)$$

Key Construction (B1) B computes, using its own private key agreement key h_B and A's public key agreement key p_A, the shared secret key as

$$K_{AB} = F(h_B, p_A)$$

As a consequence of requirement 2 of F, the two computed values for the key K_{AB} are identical.

> NOTE - This Key Agreement Mechanism has the following properties:
>
> 1. Number of passes: 0. As a consequence, the secret shared key has always the same value (but see clause 6 note 2).
>
> 2. Key authentication: this mechanism provides mutual implicit key authentication.
>
> 3. Key confirmation: this mechanism provides no key confirmation.
>
> 4. This is a key agreement mechanism since the established key is a one-way function of the private key agreement keys h_A and h_B of A and B respectively. However, one entity may know the other entity's public key prior to choosing their private key. Such an entity may select approximately s bits of the established key, at the cost of generating 2^s candidate values for their private key agreement key in the interval between discovering the other entity's public key and choosing their own private key.
>
> 5. Example: an example known as Diffie-Hellman key agreement is given in clause B.5.

6.2 Key agreement mechanism 2

This key agreement mechanism establishes in one pass a shared secret key between A and B with implicit key authentication from B to A, but no entity authentication from A to B (i.e. B does not know with whom it has established the shared secret key). The following requirements shall be satisfied:

1. Entity B has a private key agreement key h_B in H and a public key agreement key $p_B = F(h_B, g)$.
2. Entity A has access to an authenticated copy of B's public key agreement key p_B. This may be achieved using the mechanisms of clause 8.

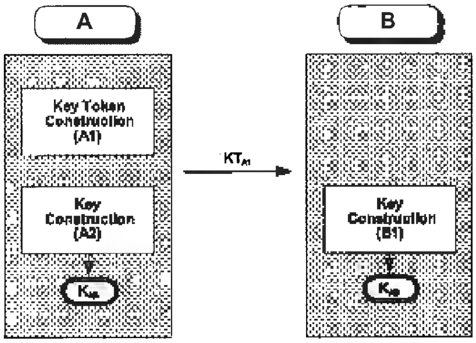


Figure 2 - Key Agreement Mechanism 2

Key Token Construction (A1) A randomly and secretly generates r in H, computes $F(r,g)$ and sends the key token

$$KT_{A1} = F(r,g) \,||\, Text$$

to B.

Key Construction (A2) Further A computes the key as

$$K_{AB} = F(r, p_B)$$

Key Construction (B1) B extracts $F(r,g)$ from the received key token KT_{A1} and computes the shared secret key

$$K_{AB} = F(h_B, F(r,g))$$

According to requirement 2 of F, the two computed values for the key K_{AB} are identical.

> NOTE - This Key Agreement Mechanism has the following properties:
>
> 1. Number of passes: 1.
>
> 2. Key authentication: this mechanism provides implicit key authentication from B to A (B is the only entity other than A who can compute the shared secret key).
>
> 3. Key confirmation: this mechanism provides no key confirmation.
>
> 4. This is a key agreement mechanism since the established key is a one-way function of a random value r supplied by A and B's private key agreement key. However, since entity A may know entity B's public key prior to choosing the value r,

entity A may select approximately s bits of the established key, at the cost of generating 2^s candidate values for r in the interval between discovering B's public key and sending KT_{A1}.

5. Example: an example of this key agreement mechanism (known as ElGamal key agreement) is described in clause B.3.

6. Key usage: as B receives the key K_{AB} from the non-authenticated entity A, secure usage of K_{AB} at B's end is restricted to functions not requiring trust in A's authenticity such as decipherment and generation of message authentication codes.

6.3 Key agreement mechanism 3

This key agreement mechanism establishes in one pass a shared secret key between A and B with mutual implicit key authentication, and entity authentication of A to B. The following requirements shall be satisfied:

1. Entity A has an asymmetric signature system (S_A, V_A).
2. Entity B has access to an authenticated copy of the public verification transformation V_A. This may be achieved using the mechanisms of clause 8.
3. Entity B has a key agreement system with keys (h_B, p_B).
4. Entity A has access to an authenticated copy of the public key agreement key p_B of entity B. This may be achieved using the mechanisms of clause 8.
5. *TVP:* The *TVP* shall either be a time stamp or a sequence number. If time stamps are used, secure and synchronized time clocks are required; if sequence numbers are used, the ability to maintain and verify bilateral counters is required.
6. The entities A and B have agreed on a cryptographic check function f (such as those standardized in ISO/IEC 9797) and a way to incorporate K_{AB} as the key in this check function.

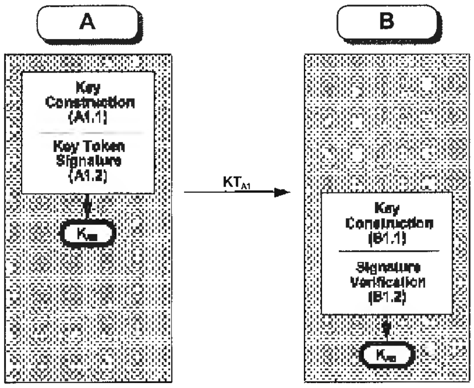


Figure 3 - Key Agreement Mechanism 3

Key Construction (A1.1) A randomly and secretly generates r in and computes $F(r,g)$. A computes the shared secret key as

$$K_{AB} = F(r,p_B)$$

Using the shared secret key K_{AB}. A computes a cryptographic check value on the concatenation of the sender's distinguishing identifier A and a sequence number or time stamp *TVP*.

Key Token Signature (A1.2) A signs the cryptographic check value, using its private signature transformation S_A. Then A forms the key token, consisting of the sender's distinguishing identifier A, the key input $F(r,g)$, the *TVP*, the signed cryptographic check value, and some optional data

$$KT_{A1} = A||F(r,g)||TVP|| \\ S_A(f_{K_{AB}}(A||TVP))||Text1$$

and sends it to B.

Key Construction (B1.1) B extracts $F(r,g)$ from the received key token and computes the shared secret key, using its private key agreement key h_B,

$$K_{AB} = F(h_B, F(r,g))$$

Using the shared secret key K_{AB} B computes the cryptographic check value on the sender's distinguishing identifier A and the *TVP*.

Signature Verification (B1.2) *B* uses the sender's public verification transformation V_A to verify *A*'s signature and thus the integrity and origin of the received key token KT_{A1}. Then *B* validates the timeliness of the token (by inspection of *TVP*).

NOTE - This Key Agreement Mechanism has the following properties:

1. Number of passes: 1.

2. Key authentication: this mechanism provides explicit key authentication from *A* to *B* and implicit key authentication from *B* to *A*.

3. Key confirmation: this mechanism provides key confirmation from *A* to *B*.

4. This is a key agreement mechanism since the established key is a one-way function of a random value *r* supplied by *A* and *B*'s private key agreement key. However, since entity *A* may know entity *B*'s public key prior to choosing the value *r*, entity *A* may select approximately *s* bits of the established key, at the cost of generating 2^s candidate values for *r* in the interval between discovering *B*'s public key and sending KT_{A1}.

5. *TVP*: provides entity authentication of *A* to *B* and prevents replay of the key token.

6. Example: an example of this key agreement mechanism (known as Nyberg-Rueppel key agreement) is described in clause B.4.

7. Public key certificates: if *Text1* is used to transfer *A*'s public key certificate, then requirement 2 at the beginning of this clause can be relaxed to the requirement that *B* is in possession of an authenticated copy of the CA's public verification key.

6.4 Key agreement mechanism 4

This key agreement mechanism establishes in two passes a shared secret key between entities *A* and *B* with joint key control without prior exchange of keying information. This mechanism provides neither entity authentication nor key authentication.

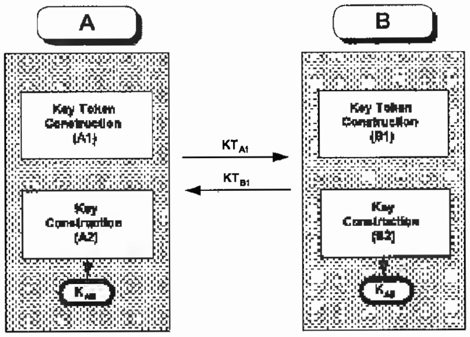


Figure 4 - Key Agreement Mechanism 4

Key Token Construction (A1) *A* randomly and secretly generates r_A in *H*, computes $F(r_A,g)$, constructs the key token

$$KT_{A1} = F(r_A,g) \,||\, Text1$$

and sends it to *B*.

Key Token Construction (B1) *B* randomly and secretly generates r_B in *H*, computes $F(r_B,g)$, constructs the key token

$$KT_{B1}= F(r_B,g) \,||\, Text2$$

and sends it to *A*.

Key Construction (A2) *A* extracts $F(r_B,g)$ from the received key token KT_{B1} and computes the shared secret key

$$K_{AB} = F(r_A,F(r_B,g))$$

Key Construction (B2) *B* extracts $F(r_A,g)$ from the received key token KT_{A1} and computes the shared secret key

$$K_{AB} = F(r_B,F(r_A,g))$$

NOTE - This Key Agreement Mechanism has the following properties:

1. Number of passes: 2.

2. Key authentication: this mechanism does not provide key authentication. However, this mechanism may be useful in environments where the authenticity of the key tokens is verified using other means. For instance, a hash-code of the key tokens may be exchanged between the entities using a second communication channel. See also Public Key

Transport Mechanism 2. Key confirmation: this mechanism provides no key confirmation.

3. This is a key agreement mechanism since the established key is a one-way function of random values r_A and r_B supplied by A and B respectively. However, since entity B may know $F(r_A, g)$ prior to choosing the value r_B, entity B may select approximately s bits of the established key, at the cost of generating 2^s candidate values for r_B in the interval between receiving KT_{A1} and sending KT_{B1}.

4. Example: an example of this mechanism (known as Diffie-Hellman key agreement) is described in clause B.5.

6.5 Key agreement mechanism 5

This key agreement mechanism establishes in two passes a shared secret key between entities A and B with mutual implicit key authentication and joint key control. The following requirements shall be satisfied:

1. Each entity X has a private key agreement key h_X in H and a public key agreement key $p_X = F(h_X,g)$.
2. Each entity has access to an authenticated copy of the public key agreement key of the other entity. This may be achieved using the mechanisms of clause 8.
3. Both entities have agreed on a common one-way function w.

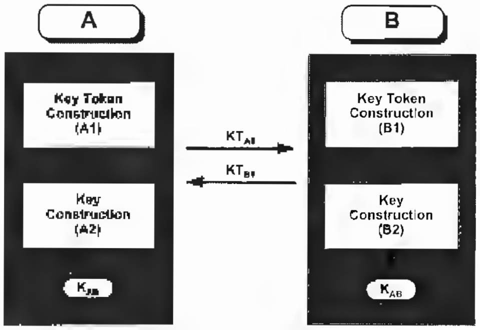


Figure 5 - Key Agreement Mechanism 5

Key Token Construction (A1) A randomly and secretly generates r_A in H, computes $F(r_A,g)$ and sends the key token

$$KT_{A1} = F(r_A,g)||Text1$$

to B.

Key Token Construction (B1) B randomly and secretly generates r_B in H, computes $F(r_B,g)$ and sends the key token

$$KT_{B1} = F(r_B,g)||Text2$$

to A.

Key Construction (B2) B extracts $F(r_A,g)$ from the received key token KT_{A1} and computes the shared secret key as

$$K_{AB} = w(F(h_B,F(r_A,g)), F(r_B,p_A))$$

where w is a one-way function.

Key Construction (A2) A extracts $F(r_B,g)$ from the received key token KT_{B1} and computes the shared secret key as

$$K_{AB} = w(F(r_A,p_B), F(h_A,F(r_B,g)))$$

NOTE - This Key Agreement Mechanism has the following properties:

1. Number of passes: 2.

2. Key authentication: this mechanism provides mutual implicit key authentication. If the data field *Text2* contains a cryptographic check value (on known data) computed using the key K_{AB}, then this mechanism provides explicit key authentication from B to A.

3. Key confirmation: if the data field *Text2* contains a cryptographic check value (on known data) computed using the key K_{AB}, then this mechanism provides key confirmation from B to A.

4. This is a key agreement mechanism since the established key is a one-way function of random values r_A and r_B supplied by A and B respectively. However, since entity B may know $F(r_A, g)$ prior to choosing the value r_B, entity B may select approximately s bits of the established key, at the cost of generating 2^s candidate values for r_B in the interval between receiving KT_{A1} and sending KT_{B1}.

5. Example: An example of this key agreement mechanism (known as the Matsumoto-Takashima-Imai A(0) key agreement scheme) is described in

clause B.6. Another example is known as the Goss protocol.

6. The function w has to hide its inputs in the sense that from the function value and from one of the inputs it is infeasible to compute the relevant part of the other input. This may be achieved by using a hash-function from ISO/IEC 10118 (there is no need for a collision-resistant hash-function).

7. Public key certificates: if *Text1* and *Text2* contain the public key certificates of entity A's and B's key agreement key, respectively, then the requirement 2 at the beginning of this clause can be replaced by the requirement that each entity is in possession of an authenticated copy of the CA's public verification key.

6.6 Key agreement mechanism 6

This key agreement mechanism establishes in two passes a shared secret key between entities A and B with mutual implicit key authentication and joint key control. It is based on the use of both an asymmetric encipherment and signature system. The following requirements shall be satisfied:

1. A has an asymmetric encipherment system with the transformations (E_A, D_A).
2. B has an asymmetric signature system with the transformations (S_B, V_B).
3. A has access to an authenticated copy of B's public verification transformation V_B. This may be achieved using the mechanisms of clause 8.
4. B has access to an authenticated copy of A's public encipherment transformation E_A. This may be achieved using the mechanisms of clause 8.

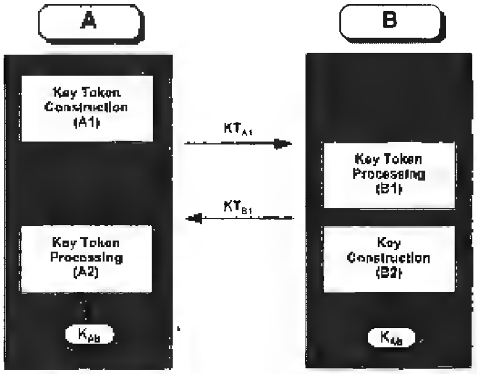

A
B
Key Token Construction (A1)
KT$_{A1}$
Key Token Processing (B1)
KT$_{B1}$
Key Token Processing (A2)
Key Construction (B2)
K$_{AB}$
K$_{AB}$

Figure 6 - Key Agreement Mechanism 6

Key Token Construction (A1) A generates a random number r_A and sends the key token

$$KT_{A1} = r_A || Text1$$

to B.

Key Token Processing (B1) B generates a random number r_B and signs a data block consisting of the distinguishing identifier A, the random number r_A, the random number r_B and some optional data *Text2* using its private signature transformation S_B

$$BS = S_B (A || r_A || r_B \ | Text2)$$

Then B enciphers a data block consisting of its distinguishing identifier B (optional), the signed block BS and some optional data *Text3*, using A's public encipherment transformation E_A, and sends the key token

$$KT_{B1} = E_A (B || BS || Text3) || Text4$$

back to A.

Key Construction (B2) The shared secret key consists of all or part of B's signature Σ contained in the signed block BS (see Notes 1 in clause 4).

Key Token Processing (A2) A deciphers the key token KT_{B1} using its private decipherment transformation D_A, optionally checks the sender identifier B, and uses B's public verification transformation V_B to verify the digital signature of the signed block BS. Then A checks the recipient identifier A and consistency of the random number r_A in the signed block BS with the random number r_A sent in token KT_{A1}. If all checks are successful, A accepts all or part of B's signature Σ of the signed block BS as the shared secret key.

NOTE - This Key Agreement Mechanism has the following properties:

1. Number of passes: 2.

2. Key authentication: this mechanism provides implicit key authentication from A to B and explicit key authentication from B to A.

3. Key confirmation: If the data field *Text3* contains a cryptographic check value (on known data) computed using the key K_{AB}, then this mechanism provides key confirmation from B to A.

4. This is a key agreement mechanism since the established key is a one-way function of random values r_A and r_B supplied by A and B respectively. However, since entity B may know $F(r_A, g)$ prior to choosing the value r_B, entity B may select approximately s bits of the established key, at the cost of generating 2^s candidate values for r_B in the interval between receiving KT_{A1} and sending KT_{B1}.

5. Example: this mechanism is derived from Beller and Yacobi's two pass protocol described in clause B.7.

6. Public key certificates: if *Text1* and *Text4* contain the public key certificate of entity A's encipherment key and the public key certificate of B's verification key, respectively, then the requirements 3 and 4 at the beginning of this clause can be relaxed to the requirement that each entity is in possession of an authenticated copy of the CA's public verification key.

7. A significant feature of this scheme is that the identity of party B may remain anonymous to eavesdroppers, of particular advantage in the wireless environment which is a main environment for the application of this scheme.

6.7 Key agreement mechanism 7

This key agreement mechanism is based on the three-pass authentication mechanism of ISO/IEC 9798-3 and establishes in three passes a shared secret key between entities A and B with mutual authentication. The following requirements shall be satisfied:

1. Each entity X has an asymmetric signature system (S_X, V_X).
2. Each entity has access to an authenticated copy of the public verification transformation of the other entity. This may be achieved using the mechanisms of clause 8.
3. Each entity has a common cryptographic check function f.

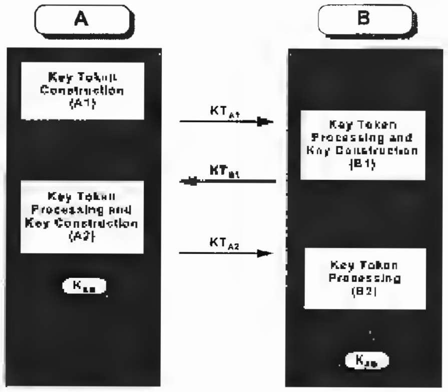

A
B
Key Token Construction (A1)
KT_{A1}
Key Token Processing and Key Construction (B1)
KT_{B1}
Key Token Processing and Key Construction (A2)
KT_{A2}
Key Token Processing (B2)
K_{AB}
K_{AB}

Figure 7 - Key Agreement Mechanism 7

Key Token Construction (A1) A randomly and secretly generates r_A in H, computes $F(r_A,g)$, constructs the key token

$$KT_{A1}= F(r_A,g) \mid\mid Text1$$

and sends it to B.

Key Token Processing and Key Construction (B1) B randomly and secretly generates r_B in H, computes $F(r_B,g)$, computes the shared secret key as

$$K_{AB}=F(r_B,F(r_A,g)),$$

constructs the signed key token

$$KT_{B1} = S_B(DB_1) \mid\mid f_{K_{AB}} (DB_1) \mid\mid Text3$$

where

$$DB_1 = F(r_B,g) \mid\mid F(r_A,g) \mid\mid A \mid\mid Text2$$

and sends it back to A.

Key confirmation is provided by sending $f_{K_{AB}}(DB_1)$ in KT_{B1}. Alternatively, if both parties have a common symmetric encryption system, key confirmation can be obtained by encrypting part of the token as follows: replace KT_{B1} by $F(r_B,g)$ followed by $E_{K_{AB}}$ $(S_B(DB_1))$.

Key Token Processing (A2) *A* verifies *B*'s signature on the key token KT_{B1} using *B*'s public verification key, verifies *A*'s distinguishing identifier and the value $F(r_A,g)$ sent in step (A1). If the check is successful, *A* proceeds to compute the shared secret key as

$$K_{AB}=F(r_A,F(r_B,g))$$

Using K_{AB}, *A* verifies the cryptographic check value $f_{K_{AB}}(DB_1)$.

Then *A* constructs the signed key token

$$KT_{A2} = S_A(DB_2) \,||\, f_{K_{AB}}(DB_2) \,||\, Text5$$

where

$$DB_2 = F(r_A,g) \,||\, F(r_B,g) \,||\, B \,||\, Text4$$

and sends it to *B*.

Key confirmation is provided by sending $f_{K_{AB}}(DB_2)$ in KT_{A2}. Alternatively, key confirmation can be obtained by encrypting part of the token as follows: replacc KT_{A2} by $E_{K_{AB}}$ $(S_A(DB_2))$.

Key Token Processing (B2) *B* verifies *A*'s signature on the key token KT_{A2}, using *A*'s public verification key, then verifies *B*'s distinguishing identifier and that the values $F(r_A,g)$ and $F(r_B,g)$ agree with the values exchanged in the previous steps. If the check is successful, *B* verifies the cryptographic check value $f_{K_{AB}}$ (DB_2) using

$$K_{AB}=F(r_B,F(r_A,g)).$$

NOTE - This Key Agreement Mechanism has the following properties:

1. Number of passes: 3.

2. Key and entity authentication: this mechanism provides mutual explicit key authentication and mutual entity authentication.

3. Key confirmation: this mechanism provides mutual key confirmation.

4. This is a key agreement mechanism since the established key is a one-way function of random values r_A and r_B supplied by *A* and *B* respectively. However, since entity *B* may know $F(r_A, g)$ prior to choosing the value r_B, entity *B* may select approximately *s* bits of the established key, at the cost of generating 2^s candidate values for r_B in the interval between receiving KT_{A1} and sending KT_{B1}.

5. Example: an example of this key agreement mechanism may be provided by the Diffie-Hellman scheme described in Annex B in conjunction with a digital signature scheme such as ISO/IEC 9796.

6. Standards: this mechanism conforms to ISO/IEC 9798-3 *Entity authentication using a public key algorithm*. KT_{A1}, KT_{B1}, and KT_{A2} are identical to the tokens sent in the three pass authentication mechanism described in subclause 5.2.2 of ISO/IEC 9798-3. Also the data fields are identical, with the following change of use:

- the data field R_A (which is present in all three tokens of ISO/IEC 9798-3, subclause 5.2.2) transmits the random function value $F(r_A,g)$
- the data field R_B (which is present in all three tokens of ISO/IEC 9798-3, subclause 5.2.2) transmits the random function value $F(r_B,g)$

7. Public key certificates: if the data fields *Text1* and *Text3* (or *Text5* and *Text3*) each contain the public key certificates of entity *A* and *B*, respectively, then the requirement 2 at the beginning of this clause can be relaxed to the requirement that all entities are in possession of an authenticated copy of the CA's public verification key.

8. Signature transformation: if a signature mechanism with text hashing is used, then $F(r_A,g)$ and/or $F(r_B,g)$ need not be sent in key token KT_{B1}. Similarly, neither $F(r_A,g)$ nor $F(r_B,g)$ need to be sent in key token KT_{A2}. However, care must be taken that the random numbers are included in the computation of the respective signatures.

7. Secret key transport

In this part of ISO/IEC 11770 key transport is the process of transferring a secret key, chosen by one entity (or a trusted center), to another entity, suitably protected by asymmetric techniques.

NOTE - In practical implementations of the key transport mechanisms the key data block may be subject to further processing prior to being used for encipherment. For instance, the key data block may be xor-ed by a (pseudo-) random bit pattern to destroy any apparent structure in the key data block.

7.1. Key transport mechanism 1

This key transport mechanism transfers in one pass a secret key from entity *A* to entity *B* with implicit key authentication from *B* to *A*. The following requirements shall be satisfied:

1. Entity *B* has an asymmetric encipherment system (E_B,D_B).
2. A has access to an authenticated copy of B's public encipherment transformation E_B. This may be achieved using the mechanisms of clause 8.
3. The optional *TVP* shall either be a time stamp or sequence number. If time stamps are used then the entities *A* and *B* need to maintain synchronous clocks or use a Trusted Third Party Time Stamp Authority. If sequence numbers are used then *A* and *B* have to maintain bilateral counters.

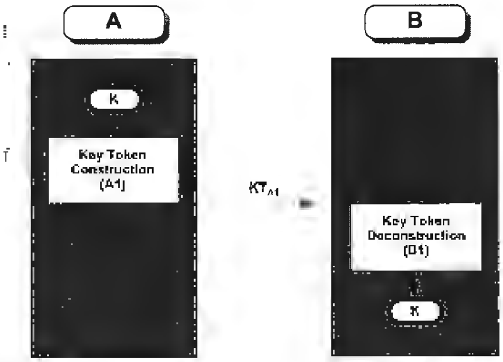


Figure 8 - Key Transport Mechanism 1

Key Token Construction (A1) *A* has obtained a key *K* and wants to transfer it securely to *B*. *A* constructs a key data block consisting of its distinguishing identifier *A* (optional), the key *K*, an optional *TVP* and an optional data field *Text1*. Then *A* encrypts the key data block using the receiver's public encipherment transformation E_B and sends the key token

$$KT_{A1} = E_B(A\,||\,K\,||TVP\,||\,Text1)\,||\,Text2$$

to *B*.

Key Token Deconstruction (B1) *B* deciphers the received key token KT_{A1} using its private decipherment transformation D_B, recovers the key *K*, checks the optional *TVP*, and associates the recovered key *K* with the claimed originator *A*.

NOTE - This Key Transport Mechanism has the following properties:

1. Number of passes: 1.

2. Key authentication: this mechanism provides implicit key authentication from *B* to *A* since only *B* can possibly recover the key *K*.

3. Key confirmation: this mechanism provides no key confirmation.

4. Key control: *A* can choose the key.

5. *TVP:* the optional *TVP* prevents the replay of the key token.

6. Key usage: as *B* receives the key *K* from the non-authenticated entity *A*, secure usage of *K* by *B* is restricted to functions not requiring trust in A's authenticity such as decipherment and generation of message authentication codes.

7. Example: an example of this mechanism (known as ElGamal key transfer) is described in clause B.8. Another example of this mechanism using RSA is described in clause B.10.

7.2. Key transport mechanism 2

This key transport mechanism is an extension of the one-pass entity authentication mechanism in ISO/IEC 9798-3. It transfers a secret key enciphered and signed from entity *A* to entity *B* with implicit key authentication from *A* to *B*. The following requirements shall be satisfied:

1. Entity *A* has an asymmetric signature system (S_A, V_A).
2. Entity *B* has an asymmetric encipherment system (E_B,D_B).
3. Entity *A* has access to an authenticated copy of *B*'s public encipherment transformation E_B. This may be achieved using the mechanisms of clause 8.
4. Entity *B* has access to an authenticated copy of *A*'s public verification transformation V_A. This may be achieved using the mechanisms of clause 8.

5. The optional *TVP* shall either be a time stamp or sequence number. If time stamps are used then the entities *A* and *B* need to maintain synchronous clocks or use a Trusted Third Party Time Stamp Authority. If sequence numbers are used then *A* and *B* have to maintain bilateral counters.

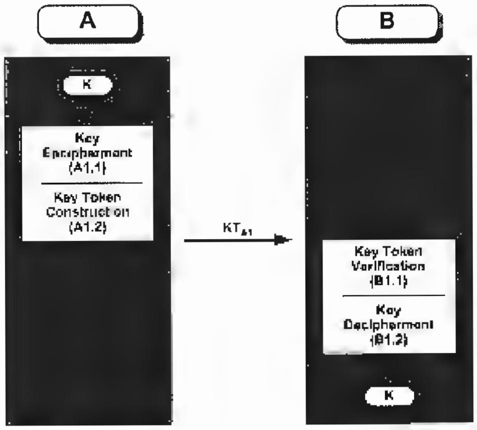


Figure 9 - Key Transport Mechanism 2

Key Encipherment (A1.1) *A* has obtained a key *K* and wants to transfer it securely to *B*. *A* forms the key data block, consisting of the sender's distinguishing identifier *A*, the key *K* and an optional data field *Text1*. Then *A* enciphers the key data block with *B*'s public encipherment transformation E_B and forms the enciphered block

$$BE = E_B(A||K||Text1)$$

Key Token Construction (A1.2) *A* forms the token data block, consisting of the recipient's distinguishing identifier *B*, an optional time stamp or sequence number *TVP*, the enciphered block *BE* and the optional data field *Text2*. Then *A* signs the token data block using its private signature transformation S_A and sends the resulting key token

$$KT_{A1} = S_A(B||TVP||BE||Text2)||Text3$$

to *B*.

Key Token Verification (B1.1) *B* uses the sender's public verification transformation V_A to verify the digital signature of the received key token KT_{A1}. Then *B* checks the receiver identification *B* and optionally the *TVP*.

Key Decipherment (B1.2) *B* deciphers the block *BE* with its private decipherment transformation D_B. Then *B* compares the field *A* in block *BE* with the identity of the signing entity. If all checks are successful, *B* accepts the key *K*.

NOTE - This Key Transport Mechanism has the following properties:

1. Number of passes: 1.

2. Key and entity authentication: this mechanism provides entity authentication of *A* to *B* if the optional *TVP* is used, and implicit key authentication from *B* to *A*.

3. Key confirmation: from *A* to *B*. *B* can be sure that it shares the correct key with *A*, but *A* can only be sure that *B* has indeed received the key after it has obtained a positive reply from *B*.

4. Key control: *A* can choose the key.

5. *TVP* (optional): provides entity authentication of *A* to *B* and prevents replay of the key token. In order to prevent replay of the key data block *BE*, an additional *TVP* may also be included in *Text1*.

6. Data field *A*: *A*'s distinguishing identifier is included in the enciphered block *BE* to prevent *A* from misappropriating an enciphered key block intended for use by another entity. This is achieved by comparing *A*'s identity with *A*'s signature on the token.

7. Standards: conformance with ISO/IEC 9798-3 *Entity authentication using a public key algorithm.* KT_{A1} is compatible to the token sent in the one-pass authentication mechanism described in subclause 5.1.1 of ISO/IEC 9798-3. The token accommodates the transfer of the key K through use of the optional text field: *Text1* has been replaced by *BE*||*Text2*.

8. Public key certificates: the data field *Text3* may be used to deliver the public key certificate of entity *A*. Then the requirement 4 at the beginning of this clause can be relaxed to the requirement that entity *B* is in possession of an authenticated copy of the CA's public verification key.

9. Mutual entity authentication and joint key control: if two executions of this key transport mechanism are combined (from *A* to *B* and from *B* to *A*) then mutual entity authentication and joint key control can be provided (depending on the use of the optional *TVP*).

10. Usage: Key transport mechanism 2 is intended to be used in environments where confidentiality of parts of a message is needed, e.g. a message that carries many non-confidential elements as well as the enciphered keys.

11. Examples of this mechanism are described in clauses B.9 and C.7.

7.3. Key transport mechanism 3

This key transport mechanism transfers in one pass a secret key signed and enciphered from entity *A* to entity *B* with unilateral key confirmation. The following requirements shall be satisfied:

1. Entity *A* has an asymmetric signature system (S_A, V_A).
2. Entity *B* has an asymmetric encipherment system (E_B, D_B).
3. Entity *A* has access to an authenticated copy of *B*'s public encipherment transformation E_B. This may be achieved using the mechanisms of clause 8.
4. Entity *B* has access to an authenticated copy of *A*'s public verification transformation V_A. This may be achieved using the mechanisms of clause 8.
5. The optional *TVP* shall either be a time stamp or a sequence number: If time stamps are used then the entities *A* and *B* need to maintain synchronous clocks. If sequence numbers are used then *A* and *B* have to maintain bilateral counters.

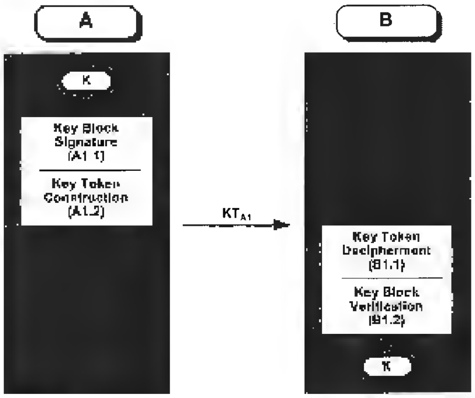

A
B
K
Key Block Signature (A1.1)
Key Token Construction (A1.2)
KT_{A1}
Key Token Decipherment (B1.1)
Key Block Verification (B1.2)
K

Figure 10 - Key Transport Mechanism 3

Key Block Signature (A1.1) *A* has obtained a key *K* and wants to transfer it securely to *B*. *A* forms a key data block consisting of the recipient's distinguishing identifier *B*, the key *K*, an optional sequence number or time stamp *TVP*, and some optional data. Then A signs the key block using its private signature transformation S_A to generate the signed block

$$BS = S_A\,(B||K||TVP||Text1)$$

Key Token Construction (A1.2) *A* forms the token data block, consisting of the signed block *BS* and some optional *Text2*. Then *A* enciphers the token data block using the receiver's public encipherment transformation E_B and sends the resulting key token

$$KT_{A1} = E_B\,(BS||\ Text2)||Text3$$

to *B*.

Key Token Decipherment (B1.1) *B* deciphers the received key token KT_{A1} using its private decipherment transformation D_B.

Key Block Verification (B1.2) *B* uses the sender's public verification transformation V_A to verify the integrity and origin of *BS*. *B* validates that it is the intended recipient of the token (by inspection of the identifier *B*) and, optionally, that the token has been sent timely (by inspection of *TVP*). If all verifications are successful, *B* accepts the key *K*.

> NOTE - This Key Transport Mechanism has the following properties:
>
> 1. Number of protocol passes: 1.

2. Key and entity authentication: this mechanism provides entity authentication of A to B if the optional TVP is used, and implicit key authentication from B to A.

3. Key confirmation: from A to B. B can be sure that it shares the correct key K with A, but A can only be sure that B has indeed received the key after it has obtained a positive reply from B.

4. Key control: A can choose the key.

5. TVP (optional): may provide entity authentication of A to B and prevent replay of the key token.

6. Data field B: B's distinguishing identifier is included in the signed key block BS to explicitly indicate the recipient of the key, thereby preventing misuse of the signed block BS by B.

7. Public key certificates: the data field *Text3* may be used to deliver the public key certificate of entity A. Then the requirement 4 at the beginning of this clause can be relaxed to the requirement that entity B is in possession of an authenticated copy of the CA's public verification key.

8. Mutual entity authentication and joint key control: if two executions of this key transport mechanism are combined (from A to B and from B to A) then mutual entity authentication and joint key control can be provided (depending on the use of the optional TVP).

7.4. Key transport mechanism 4

This key transport mechanism is based on the two-pass authentication mechanism of ISO/IEC 9798-3 and transfers a key from entity B to A. The following requirements shall be satisfied:

1. Entity A has an asymmetric encipherment system (E_A,D_A).
2. Entity B has an asymmetric signature system (S_B,V_B).
3. Entity A has access to an authenticated copy of B's public verification transformation V_B. This may be achieved using the mechanisms of clause 8.
4. Entity B has access to an authenticated copy of A's public encipherment transformation E_A. This may be achieved using the mechanisms of clause 8.

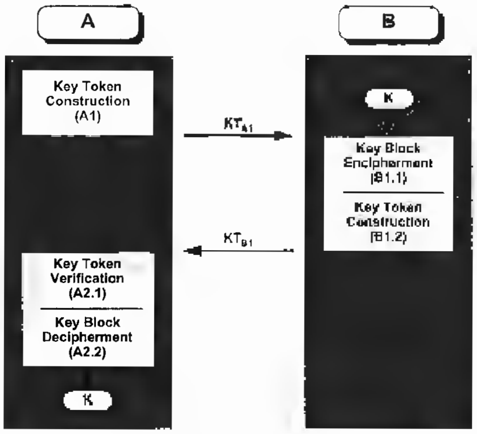

A
B
Key Token Construction (A1)
K
KT_A1
Key Block Encipherment (B1.1)
Key Token Construction (B1.2)
KT_B1
Key Token Verification (A2.1)
Key Block Decipherment (A2.2)
K

Figure 11 - Key Transport Mechanism 4

Key Token Construction (A1) A constructs the key token KT_{A1}, consisting of a random number r_A and an optional data field *Text1*,

$$KT_{A1} = r_A || Text1$$

and sends it to B.

Key Block Encipherment (B1.1) B has obtained a key K and wants to transfer it securely to A. B forms a key data block, consisting of the sender's distinguishing identifier B, the key K and an optional data field *Text2*. Then B enciphers the key data block with A's public encipherment transformation E_A and forms the enciphered block

$$BE = E_A (B||K||Text2)$$

Key Token Construction (B1.2) B forms the token data block, consisting of the recipient's distinguishing identifier A, the random number r_A received in step (A1), the new random number r_B (optional), the enciphered block BE, and the optional data field *Text3*. Then B signs the token data block with its private signature transformation S_B and sends the resulting key token

$$KT_{B1} = S_B (A||r_A||r_B||BE||Text3)||Text4$$

to A.

Key Token Verification (A2.1) *A* uses the sender's public verification transformation V_B to verify the digital signature of the received key token KT_{B1}. Then *A* checks the distinguishing identifier *A* and checks that the received value r_A agrees with the random number sent in step (A1).

Key Block Decipherment (A2.2) *A* deciphers the block *BE* with its private decipherment transformation D_A. Then *A* validates the sender's distinguishing identifier *B*. If all checks are successful, *A* accepts the key *K*.

> NOTE - This Key Transport Mechanism has the following properties:
>
> 1. Number of protocol passes: 2.
>
> 2. Key and entity authentication: this mechanism provides entity authentication of *B* to *A* and implicit key authentication from *A* to *B*.
>
> 3. Key confirmation: from *B* to *A*. *A* can be sure that it shares the correct key *K* with *B*, but *B* can only be sure that *A* has indeed received the key after it has obtained a secured message from *A* which has been unambiguously processed.
>
> 4. Key control: *B* can choose the key.
>
> 5. Standards: conformance with ISO/IEC 9798-3 *Entity authentication using a public key algorithm.* The tokens KT_{A1} and KT_{B1} are compatible with the tokens sent in the two-pass authentication mechanism described in subclause 5.1.2 of ISO/IEC 9798-3 (note that the roles of *A* and *B* are exchanged). The token KT_{B1} accommodates the transfer of the key *K* through use of the optional data field: *Text2* has been replaced by *BE*| *Text3*.
>
> 6. Standards: if this key transport mechanism is executed twice in parallel between two entities, then the resulting mutual key transport mechanism is in conformance with the mechanism described in subclause 5.2.3. *Two pass parallel authentication* of ISO/IEC 9798-3.
>
> 7. Data field r_B: is shown for consistency with ISO/IEC 9798-3. Because of the presence of *BE* in KT_{B1} the data field r_B is no longer required and is therefore optional in this mechanism.
>
> 8. Mutual entity authentication and joint key control: if two executions of this key transport mechanism are combined (from *A* to *B* and from *B* to *A*) then mutual entity authentication and joint key control can be provided.

7.5. Key transport mechanism 5

This key transport mechanism is based on the three-pass authentication mechanism of ISO/IEC 9798-3 and transfers in three passes two shared secret keys with mutual entity authentication and key confirmation. One key is transferred from *A* to *B* and one key from *B* to *A*. The following requirements shall be satisfied:

1. Each entity *X* has an asymmetric signature system (S_X, V_X).
2. Each entity *X* has an asymmetric encipherment system (E_X, D_X).
3. Each entity has access to an authenticated copy of the public verification transformation of the other entity. This may be achieved using the mechanisms of clause 8.
4. Each entity has access to an authenticated copy of the public encipherment transformation of the other entity. This may be achieved using the mechanisms of clause 8.

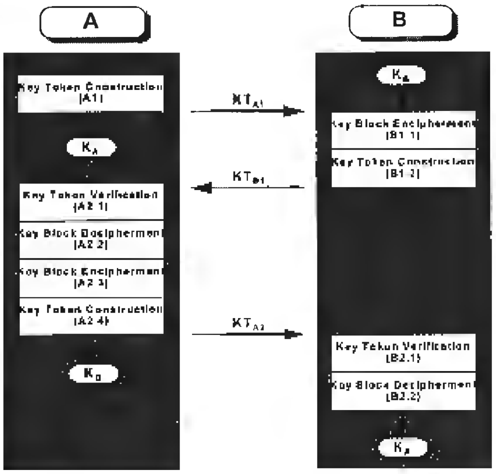

A
B
Key Token Construction (A1)
K_A
Key Token Verification (A2.1)
Key Block Decipherment (A2.2)
Key Block Encipherment (A2.3)
Key Token Construction (A2.4)
K_B
KT_{A1}
KT_{B1}
KT_{A2}
K_B
Key Block Encipherment (B1.1)
Key Token Construction (B1.2)
Key Token Verification (B2.1)
Key Block Decipherment (B2.2)
K_A

Figure 12 - Key Transport Mechanism 5

Key Token Construction (A1) A randomly generates r_A and constructs the key token

$$KT_{A1} = r_A||Text1$$

and sends it to B.

Key Block Encipherment (B1.1) B has obtained a key K_B and wants to transfer it securely to A. B constructs a block containing its own distinguishing identifier B, the kcy K_B, and some optional *Text2*, and enciphers the block, using the recipient's public encipherment transformation E_A

$$BE_1 = E_A(B||K_B||Text2)$$

Key Token Construction (B1.2) Then B randomly generates r_B and constructs a data block, containing r_B, r_A, the recipient's identity A, the enciphered key block BE_1, and some optional *Text3*. B signs the block using its private signature transformation S_B, and sends the key token

$$KT_{B1} = S_B(r_B||r_A||A||BE_1||Text3)||Text4$$

to A.

Key Token Verification (A2.1) A vcrifies B's signaturc on the key token KT_{B1} using B's public verification transformation V_B, checks the distinguishing identifier A and checks that the received value r_A agrees with the random number sent in step (A1).

Key Block Decipherment (A2.2) A deciphers thc enciphered block BE_1 using its private decipherment transformation D_A and checks the distinguishing identifier B. If all checks are successful, A accepts the key K_B.

Key Block Encipherment (A2.3) Then A constructs a data block, containing its own distinguishing identifier A, its own key K_A, and some optional *Text5*, and enciphers the block, using the recipient's public encipherment transformation E_B

$$BE_2 = E_B(A||K_A||Text5)$$

Key Token Construction (A2.4) Then A constructs a data block, containing the random number r_A, the random number r_B, the recipient's distinguishing identifier B, the enciphered key block BE_2, and some optional *Text6*. A signs the data block using its private signature transformation S_A, and sends the key token

$$KT_{A2} = S_A(r_A||r_B||B||BE_2||Text6)||Text7$$

to B.

Key Token Verification (B2.1) B verifies A's signature on the key token KT_{A2}, using A's public verification transformation V_A, checks the distinguishing identifier B and checks that the received value r_B agrees with thc random number sent in step (B1.2). In addition, B checks that the received value r_A agrees with the one contained in KT_{A1}.

Key Block Decipherment (B2.2) B deciphers the enciphered block BE_2 using its private decipherment transformation D_B and verifies the distinguishing identifier A. If all checks are successful, B accepts the key K_A.

If only unilateral key transport is required then as appropriate either BE_1 or BE_2 can be omitted.

NOTE - This Key Transport Mechanism has the following properties:

1. Number of passes: 3.

2. Key and entity authentication: this mechanism provides mutual entity authentication, implicit key authentication of K_A from B to A and implicit key authentication of K_B from A to B.

3. Key confirmation: this mechanism provides key confirmation from sender to recipient for both keys K_A and K_B. Moreover, if A includes a cryptographic check value on K_B in the data field *Text6* of KT_{A2}, then this mechanism providcs mutual key confirmation with respect to K_B.

4. Key control: A can choose the key K_A, since it is the originating entity. Similarly, B can choose the key K_B. Joint key control can be achieved by each entity by combining the two keys K_A and K_B on both sides to form a shared secret key K_{AB}. However, the combination function must be one-way, otherwise A can choose the shared secret key. This mechanism could then be classified as a key agreement mechanism.

5. Standards: conformance to ISO/IEC 9798-3, KT_{A1}, KT_{B1}, and KT_{A2} are compatible to the tokens sent in the three pass authentication mechanism described in clause 5.2.2 of ISO/IEC 9798-3. The second token accommodates the transfer of the key K_B: *Text2* has been replaced by $BE_1||Text3$. The third token accommodates the transfer of the key K_A: *Text4* has been replaced by $BE_2||Text6$. The

third token may also accommodate the transfer of a cryptographic check value within *Text6*.

6. Public key certificates: if the data fields *Text1* and *Text4* (or *Text7* and *Text4*) each contain the public key certificates of entity *A* and *B*, respectively, then the requirement 3 and 4 at the beginning of this clause can be relaxed to the requirement that all entities are in possession of an authenticated copy of the CA's public verification key.

7. Signature transformation: if a signature mechanism with text hashing is used, then optionally the random number r_A need not be sent in the key token KT_{B1}. Analogously, neither r_A nor r_B need to be sent in key token KT_{A2} . However, carc must be taken that the random numbers are included in the computation of the respective signatures.

7.6. Key transport mechanism 6

This key transport mechanism securely transfers in three passes two secret keys, one from *A* to *B* and one from *B* to *A*. In addition, the mechanism provides mutual entity authentication and mutual key confirmation about their respective keys. This mechanism is based on the following requirements:

1. Each entity *X* has an asymmetric encipherment system (E_X, D_X).
2. Each entity has access to an authenticated copy of the public encipherment transformation of the other entity. This may be achieved using the mechanisms of clause 8.

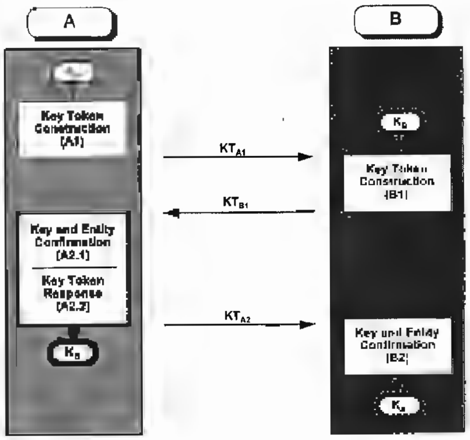

A
B
Key Token Construction [A1]
K_B
KT_{A1}
Key Token Construction [B1]
KT_{B1}
Key and Entity Confirmation [A2.1]
Key Token Response [A2.2]
KT_{A2}
Key and Entity Confirmation [B2]
K_B
K_A

Figure 13 - Key Transport Mechanism 6

Key Token Construction (A1) *A* has obtained a key K_A and wants to transfer it securely to *B*. *A* selects a random number r_A and constructs a key data block consisting of its distinguishing identifier *A*, the key K_A, the number r_A and an optional data field *Text1*. Then *A* enciphers the key block using *B*'s public encipherment transformation E_B, thereby producing the enciphered data block

$$BE_1 = E_B(A||K_A||r_A||Text1)$$

A constructs the token KT_{A1}, consisting of the enciphered data block and some optional data field *Text2*

$$KT_{A1} = BE_1||Text2$$

A sends the token to *B*.

Key Token Construction (B1) *B* cxtracts the enciphered key block BE_1 from the received key token KT_{A1} and deciphers it using its private decipherment transformation D_B. Then *B* verifies the sender identity *A*.

B has obtained a key K_B and wants to transfer it securely to *A*. *B* selects a random number r_B and constructs a key data block consisting of the distinguishing identifier *B*, the key K_B, the random number r_B, the random number r_A (as extracted from the deciphered block) and an optional data field *Text3*. Then *B* enciphers the key block using *A*'s public encipherment transformation E_A, thereby producing the enciphered data block

$$BE_2 = E_A (B \,||\, K_B \,||r_A \,||r_B \,||Text3)$$

Then B constructs the key token KT_{B1}, consisting of the enciphered data block BE_2 and an optional data field *Text4*,

$$KT_{B1} = BE_2||Text4$$

B sends the token to A.

Key and Entity Confirmation (A2.1) A extracts the enciphered key block BE_2 from the received key token KT_{B1} and deciphers it using its private decipherment transformation D_A. Then A checks the validity of the key token through comparison of the random number r_A with the random number r_A contained in the enciphered block BE_2. If the verification is successful, A has authenticated B and at the same time obtained confirmation that K_A has safely reached entity B.

Key Token Response (A2.2) A extracts the random number r_B from the deciphered key block and constructs the key token KT_{A2}, consisting of the random number r_B and an optional data field *Text5*,

$$KT_{A2} = r_B \,||Text5.$$

A sends the token to B.

Key and Entity Confirmation (B2) B verifies that the response r_B extracted from KT_{A2} is consistent with the random number r_B sent in enciphered form in KT_{B1}. If the verification is successful, B has authenticated A and at the same time has obtained confirmation that K_B has safely reached entity B.

NOTE - This Key Transport Mechanism has the following properties:

1. Number of passes: 3.

2. Entity authentication: this mechanism provides mutual entity authentication, implicit key authentication of K_A from B to A and implicit key authentication of K_B from A to B..

3. Key confirmation: this mechanism provides mutual key confirmation.

4. Key control: A can choose the key K_A, since it is the originating entity. Similarly, B can choose the key K_B. Joint key control can be achieved by each entity by combining the two keys K_A and K_B on both sides to form a shared secret key K_{AB}. However, the combination function must be one-way, otherwise B can choose the shared secret key. This mechanism could then be classified as a key agreement mechanism.

5. Key usage: this mechanism uses asymmetric techniques to mutually transfer two secret keys, K_A from A to B and K_B from B to A. The following cryptographic function separation may be derived from the mechanism: A uses its key K_A to encipher messages for B and to verify authentication codes from B. B in turn uses the received key K_A to decipher messages from A and generate authentication codes for A. The cryptographic functions of K_B may be separated in an analogous manner. In such a way, the asymmetric basis of the key transport mechanism may be extended to the usage of the secret keys.

6. Example: this mechanism is derived from the three pass protocol known as COMSET (see Brandt et al. in the Bibliography).

7. Background: this mechanism is based on zero-knowledge techniques. From the execution of the mechanism neither of the entities learns anything that it could not have computed itself.

8. Public key transport

This clause describes key management mechanisms that make an entity's public key available to other entities in an authenticated fashion. Authenticated distribution of public keys is an essential security requirement. This authenticated distribution can be achieved in different ways:

1. Public key distribution without a trusted third party;
2. Public key distribution involving a trusted third party such as a certification authority.

The public key of an entity A is part of the public key information of A. The public key information includes at least A's distinguishing identifier and A's public key.

8.1. Public key distribution without a trusted third party

This subclause describes mechanisms which provide authenticated distribution of public keys without the involvement of a trusted third party.

8.1.1 Public key transport mechanism 1

If A has access to a protected channel (i.e. a channel which provides data origin authentication and data integrity) such as a courier, registered mail, etc., to B then A may transport its public key information directly via that protected channel to B. This is the most elementary form of transferring a public key. The following requirements shall be satisfied:

1. Entity A's public key information PKI_A contains at least A's distinguishing identifier and A's public key. In addition it may contain a serial number, a validity period, a time stamp and other data elements.
2. Since the public key information PKI does not contain any secret data, the communication channel need not provide confidentiality.

Key Token Construction (A1) A constructs the key token KT_{A1} containing the public key information of A and some optional data field *Text*, and sends it via a protected channel to B.

$$KT_{A1} = PKI_A \,||\, Text$$

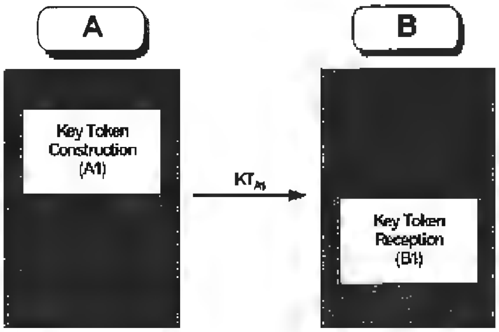


Figure 14 - Public Key Transport Mechanism 1

Key Token Reception (B1) B receives the key token via the protected channel from A, retrieves A's public key information PKI_A and stores A's public key into the list of active public keys (this list shall be protected from tampering).

NOTE - This Public Key Transport Mechanism has the following properties:

1. This mechanism can be used to transfer public verification keys (for an asymmetric signature system) or public encipherment keys (for an asymmetric encipherment system) or public key agreement keys.

2. Authentication in this context includes both data integrity and data origin authentication (as defined in ISO 7498-2:1989).

8.1.2 Public key transport mechanism 2

This mechanism transports the public key information of entity A via an unprotected channel to B. To verify the integrity and the origin of the received public key information a second authenticated channel is used. Such a mechanism is useful when the public key information PKI is transferred electronically on a high bandwidth channel, whereas the authentication of thc public key information takes place over an authenticated low bandwidth channel such as a telephone, courier, registered mail. As an additional requirement the entities shall share a common hash-function *hash*, as defined in ISO/IEC 10118-1. The following requirements shall be satisfied:

1. Entity A's public key information PKI_A contains at least A's distinguishing identifier and A's public key. In addition it may contain a serial number, a validity pcriod, a time stamp and other data elements.
2. Since the public key information PKI does not contain any secret data, thc communication channel need not provide confidentiality.

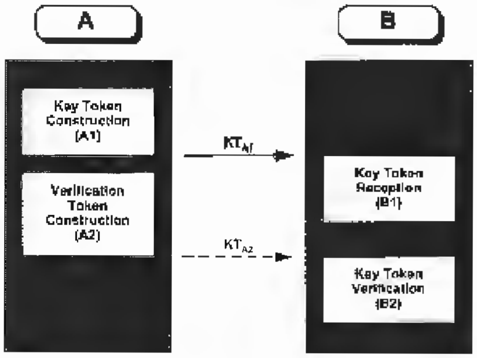

A
B
Key Token Construction (A1)
Verification Token Construction (A2)
KT_A1
KT_A2
Key Token Reception (B1)
Key Token Verification (B2)

Figure 15 - Public Key Transport Mechanism 2

Key Token Construction (A1) A constructs the key token KT_{A1} containing the public key information of A and sends it to B.

$$KT_{A1} = PKI_A \mid Text1$$

Key Token Reception (B1) B receives the key token, retrieves A's public key information PKI_A, optionally, verifies A's verification key, and stores it protected from tampering for later verification and use.

Verification Token Construction (A2) A computes a check value $hash(PKI_A)$ on its public key information and sends this check value together with the optional distinguishing identifiers of A and B to entity B using a second independent and authenticated channel (e.g. a courier or registered mail).

$$KT_{A2} = A \,||\, B \,||\, hash(PKI_A) \,||\, Text2$$

Key Token Verification (B2) Upon reception of the verification token KT_{A2}, B optionally checks the distinguishing identifier of A and B, computes the check value on the public key information of A received in the key token KT_{A1} and compares it with the check value received in the verification token KT_{A2}. If the check succeeds, B puts A's public key into the list of active public keys (this list shall be protected from tampering).

NOTE - This Public Key Transport Mechanism has the following properties:

1. This mechanism can be used to transfer public verification keys (for an asymmetric signature system) or public encipherment keys (for an asymmetric encipherment system) or public key agreement keys.

2. Authentication in this context includes both data integrity and data origin authentication.

3. If the public key that is transported is a key for an asymmetric signature system not giving message recovery, then A may sign the token KT_{A1} using the corresponding private signature key. In that case, the verification of A's signature in step (B1) using the received public verification key confirms that A knew the corresponding private signature key, and so presumably, was the only entity that knew the corresponding private signature key at the time the token was created. If a time stamp is used in PKI, then verification confirms that A currently knows the corresponding private signature key.

4. A manually signed letter may be used for the verification token.

8.2. Public key distribution using a trusted third party

The authentication of the entities' public keys can be ensured by exchanging the public keys in the form of public key certificates. A public key certificate contains the public key information, together with a digital signature provided by a trusted third party, the Certification Authority (CA). The introduction of a CA reduces the problem of authenticated user public key distribution to the problem of authenticated distribution of the CA's public key, at the expense of a trusted centre (the CA), see reference ISO/IEC 9594-8, 11770-1 (Annex D).

8.2.1 Public key transport mechanism 3

This mechanism transfers a public key from entity A to entity B in an authenticated way. It is based on the assumption that a valid public key certificate $Cert_A$ of A's public key information PKI_A has been issued by some certification authority, and that B has access to an authenticated copy of the public verification transformation V_{CA} of that certification authority CA which has issued the public key certificate.

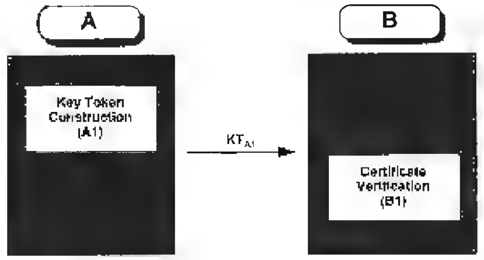


Figure 16 - Public Key Transport Mechanism 3

Key Token Construction (A1) *A* constructs the key token KT_{A1} containing the public key certificate of *A* and sends it to *B*.

$$KT_{A1} = Cert_A \,||\, Text$$

Certificate Verification (B1) Upon reception of the public key certificate, *B* uses the public verification transformation V_{CA} of the certification authority to verify the authenticity of the public key information and to check the validity of *A*'s public key.

If *B* wants to make sure that *A*'s public key certificate has not been revoked recently, then *B* should consult a trusted third party (such as the CA) via some authenticated channel.

NOTE - This Public Key Transport Mechanism has the following properties:

1. Number of passes: 1. But there may have been a request from *B* to *A* for the transfer of the public key certificate. This additional pass is optional and not shown here. *A*'s public key certificate could also be distributed by a directory in which case this public key transport mechanism would be executed between the directory and *B*.

2. Entity authentication: entity authentication is not provided by this mechanism.

3. Key confirmation: receiving a public key certificate provides confirmation that the public key has been certified by the CA.

4. The public verification key v_{CA} of the CA shall be made available to *B* in an authenticated way. This can be done using the mechanisms described in clause 8.

Annex A
(informative)

Properties of key establishment mechanisms

The following tables summarize the major properties of the key establishment/transport mechanisms specified in this part of ISO/IEC 11770.

The following notation is used:

A	the mechanism provides the property with respect to entity *A*.
A,B	the mechanism provides the property with respect to both entities, *A* and *B*.
no	the mechanism does not provide the property.
opt	the mechanism can provide the property as an option, using additional means.
(*A*)	the mechanism can optionally provide the property with respect to entity *A*, using additional means.

Public key operations: the number of computations of asymmetric transformation, e.g., "2,1" means that entity *A* needs two computations of the function *F* and *B* needs one computation of the function *F* in Key Agreement Mechanism 2.

Properties of Key Agreement Mechanisms:

Mechanism	1	2	3	4	5	6	7
Number of passes	0	1	1	2	2	2	3
Implicit key authentication	*A,B*	*B*	*A,B*	no	*A,B*	*A,B*	*A,B*
Key confirmation	no	no	B	no	opt	opt	*A,B*
Entity authentication	no	no	(*A*)	no	no	*B*	*A,B*
Public key operations	1,1	2,1	3 (or 2),2	2,2	2,2	2,2	3,3

Properties of Key Transport Mechanisms:

Mechanism	1	2	3	4	5	6
Number of passes	1	1	1	2	3	3
Implicit key authentication	*B*	*B*	*B*	*A*	*A,B*	*A,B*
Key confirmation	no	*B*	*B*	*A*	(*A*),*B*	*A,B*
Key control	*A*	*A*	*A*	*B*	*A* resp. *B*	(*A*),*B*
Entity authentication	no	(*A*)	(*A*)	*B*	*A,B*	*A,B*
Public key operations	1,1	2,2	2,2	4,4	4,4	2,2

Annex B
(informative)

Examples of key establishment mechanisms

This informative annex gives examples of some of the key establishment mechanisms described in this part of ISO/IEC 11770.

We first specify a widely used example of a function F, and accompanying sets G and H, which is conjectured to satisfy the five properties listed in clause 6, given that certain parameters are chosen appropriately.

Let p be a prime number, G be the set of elements of the Galois field with p elements, F_p, and let $H = \{1, \ldots, p\text{-}2\}$. Let g be a primitive element of F_p. Then set

$$F(h,g) = g^h \bmod p$$

F is commutative with respect to h

$$(g^{h_B})^{h_A} = (g^{h_A})^{h_B} = g^{h_A h_B} \bmod p$$

The prime p must be large enough so that $F(\cdot,g)$ can be conjectured to be a one-way function. Let each entity X have a private key h_X in H, which is only known by X, and a public key $p_X = g^{h_X} \bmod p$ known by all other entities.

> NOTE - On the selection of parameters.
>
> For discrete logarithm modulo a prime: The size of the prime should be chosen such that computing discrete logarithms in the corresponding cyclic group is computationally infeasible. Some other conditions on the prime number may be imposed in order to make discrete logarithms infeasible.
>
> It is recommended to either choose p to be a strong prime such that $p\text{-}1$ has a large prime factor or to choose g to be a generator of a group of large prime order q.
>
> For discrete logarithm modulo a composite: The modulus should be chosen as the product of two distinct odd primes that should be kept secret. The size of the modulus should be chosen such that factoring the modulus is computationally infeasible. Some additional conditions on the choice of the primes may be imposed in order to make factoring the modulus computationally infeasible.

B.1. Non-interactive Diffie-Hellman key agreement

This [6] is an example of Key Agreement Mechanism 1.

Key Construction (A1) A computes, using its own private key agreement key h_A and B's public key agreement key p_B, the shared key as

$$K_{AB} = p_B^{\ h_A} \bmod p$$

Key Construction (B1) B computes, using its own private key agreement key h_B and A's public key agreement key p_A, the shared key as

$$K_{AB} = p_A^{\ h_B} \bmod p$$

B.2. Identity-based mechanism

This [8] is an example of Key agreement Mechanism 1, which is identity-based in the following sense:

- the public key of an entity can be retrieved from some combination of its identity and its certificate;

- the authenticity of the certificate is not directly verified, but the correct public key can only be recovered from an authentic certificate.

Let (n,y) be the public verification key of a certification authority, in the digital signature scheme giving message recovery specified in ISO/IEC 9796, Annex A (informative). Therefore n is the product of two large prime numbers p and q, kept secret by the certification authority, and y is co-prime with lcm($p\text{-}1$, $q\text{-}1$).

Let O be an integer of large order modulo n and $g = O^y \bmod n$.

Let I_X be the result of adding redundancy (as specified in ISO/IEC 9796) to a public information on entity X which contains at least the distinguished identifier of X and possibly a serial number, a validity period, a time stamp and other data elements. Then *X*'s key management pair is (h_X, p_X) where h_X is an integer less than n and

$$p_X = g^{h_X} (\mathrm{mod}\, n).$$

Its certificate is computed by the certification authority as

$$Cert_X = s_X\, O^{h_X}\ (\mathrm{mod}\ n),$$

where s_X is the integer such that:

$$s_X^{y}\, I_X = 1\ (\mathrm{mod}\ n)$$

Key Construction (A1) *A* computes the public key of *B* as

$$p_B = Cert_B^{\ y} . I_B \ \mathrm{mod}\ n$$

and computes the shared secret key as

$$K_{AB} = p_B^{\ h_A} = g^{h_A h_B}\ \mathrm{mod}\ n$$

Key Construction (B1) *B* computes the public key of *A* as

$$p_A = Cert_A^{\ y} . I_A \ \mathrm{mod}\ n$$

and computes the shared secret key as

$$K_{AB} = p_A^{\ h_B} = g^{h_A h_B}\ \mathrm{mod}\, n$$

> NOTE - A one-pass and a two-pass identity-based mechanisms using the same set-up are described in the references [8], [19] and [20] of the Annex D (Bibliography).

B.3. ElGamal key agreement

This [7] is an example of Key Agreement Mechanism 2.

One shall check that p to be a strong prime such that $p\text{-}1$ has a large prime factor and that the exponentials are not of the form 0, +1, −1 mod p.

Key Token Construction (A1) *A* randomly and secretly generates r in $\{1, \dots, p\text{-}2\}$, computes g^r mod p and constructs the key token

$$KT_{A1} = g^r \ \mathrm{mod}\ p$$

and sends it to *B*.

Key Construction (A2) *A* computes the shared key

$$K_{AB} = (p_B)^{\ r}\ \mathrm{mod}\ p = g^{\ h_B r}\ \mathrm{mod}\ p$$

Key Construction (B1) *B* computes the shared key

$$K_{AB} = (g^{\ r})^{\ h_B} = g^{\ h_B r}\ \mathrm{mod}\ p$$

B.4. Nyberg-Rueppel key agreement

This [18] is an example of Key Agreement Mechanism 3. The signature system and the key agreement system are chosen in such a way that the signature system is determined by the keys (h_X, p_X).

Let q be a large prime divisor of p-1, g an element of F_p of order q, and set $H = \{1, \dots, q\text{-}1\}$. Then *X*'s asymmetric key pair used for signatures and key agreements is (h_X , p_X), where h_X is an element of H and

$$p_X = g^{h_X} \mathrm{mod}\, p$$

To prevent replay of old key tokens this example makes use of a time-stamp or a serial number, *TVP*, and of a cryptographic hash function *hash*, which maps strings of bits of arbitrary length to random integers in a large subset of $\{1, \dots, p\text{-}1\}$, for example, in *H*.

Key Construction (A1.1) *A* randomly and secretly generates r in H and computes

$$e = g^r \mathrm{mod}\, p$$

Further *A* computes the shared secret key as

$$K_{AB} = p_B^{\ r}\ \mathrm{mod}\ p$$

Using the shared secret key K_{AB} *A* computes a cryptographic check value on the sender's distinguished identifier *A* and a sequence number or time-stamp *TVP*.

$$e' = e\ hash(K_{AB} || A || TVP)\ \mathrm{mod}\ p$$

Key Token Signature (A1.2) *A* computes the signature

$$y = r - h_A\, e'\ \mathrm{mod}\ q$$

A forms the key token

$$KT_{A1} = A||e||TVP||y$$

and sends it to B.

Key Construction (B1.1) B computes the shared secret key, using its private key agreement key h_B,

$$K_{AB} = e^{h_B} \bmod p$$

Using the shared secret key K_{AB} B computes the cryptographic check value on the sender's distinguished identifier A and the TVP, and computes

$$e' = e\ hash(K_{AB}||A||TVP) \bmod p$$

Signature Verification (B1.2) B checks the validity of TVP and verifies, using the sender's public key p_A, the equality

$$e = g^y {p_A}^{e'} \bmod p$$

B.5. Diffie-Hellman key agreement

This [6] is an example of Key Agreement Mechanism 4.

One shall check that p to be a strong prime such that p-1 has a large prime factor and that the exponentials are not of the form 0, +1, -1 mod p.

Key Token Construction (A1) A randomly and secretly generates r_A in $\{1, \ldots, p\text{-}2\}$, computes g^{r_A} mod p, constructs the key token

$$KT_{A1} = g^{r_A} \bmod p$$

and sends it to B.

Key Token Construction (B1) B randomly and secretly generates r_B in $\{1, \ldots, p\text{-}2\}$, computes g^{r_B} mod p, constructs the key token

$$KT_{B1} = g^{r_B} \bmod p$$

and sends it to A.

Key Construction (A2) A computes the shared key

$$K_{AB} = (g^{r_B})^{r_A} = g^{r_A r_B} \bmod p$$

Key Construction (B2) B computes the shared key

$$K_{AB} = (g^{r_A})^{r_B} = g^{r_A r_B} \bmod p$$

B.6. Matsumoto-Takashima-Imai A(0) key agreement

This [1] is an example of Key Agreement Mechanism 5.

One recommended method is to use a safe prime p and to check that the exponentials are not of the form 0, +1, −1 mod p.

Key Token Construction (A1) A randomly and secretly generates r_A in $\{1, \ldots, p\text{-}2\}$, computes the key token

$$KT_{A1} = g^{r_A} \bmod p$$

and sends it to B.

Key Token Construction (B1) B randomly and secretly generates r_B in $\{1, \ldots, p\text{-}2\}$, computes the key token

$$KT_{B1} = g^{r_B} \bmod p$$

and sends it to A.

Key Construction (B2) B computes the shared key as

$$K_{AB} = w({KT_{A1}}^{h_B}, {p_A}^{r_B}) = {KT_{A1}}^{h_B} {p_A}^{r_B} \bmod p$$

Key Construction (A2) A computes the shared key as

$$K_{AB} = w({p_B}^{r_A}, {KT_{B1}}^{h_A}) = {KT_{A1}}^{h_B} {p_A}^{r_B} \bmod p$$

B.7. Beller-Yacobi Protocol

This part of the Annex gives a description of the original Beller-Yacobi protocol [4], which has been used to derive Key Agreement Mechanism 6.

Note: This mechanism is not completely compatible with the Mechanism 6 as it was optimized for specific situations. Specifically it uses ElGamal signature scheme and makes use of an additional symmetric encryption algorithm to transfer B's signature verification key and its certificate to A in a confidential way, thus assuring anonymity.

Let *enc:* K⎕$M \rightarrow C$ be a conventional encryption function, such as DES, where K = key space, M = message space, and C = cryptogram space.

Let S_X denote the ElGamal signature operation of entity X. The process described below emphasizes the distinction between off-line and on-line operations required in EG family of signature schemes.

We use P_X and C_X to denote entity X's public key and certificate, respectively. The public encryption operation of entity X (which uses P_X) is denoted E_X (modular squaring in the case of Rabin).

Off-line computation: B picks a random number r_B and computes

$$u = g^{r_B} \bmod p$$

Key Token Construction (A1): A picks a random number r_A and computes

$$KT_{A1} = (r_A \| A \| C_A)$$

and sends it to B.

Key Token Processing (B1) B produces the signature

$$BS = (u, v) = S_B(r_A \| A),$$

Then B picks a random x_B and creates

$$KT_{B1} = E_A(BS) \| enc(u, (B \| P_B \| C_B \| x_B))$$

and sends it to A.

Key Construction (B2) The shared secret key consists of part of B's signature, u.

Entity Authentication and Key Construction (A2) A deciphers the key token $E_A(BS)$ to find the session key u, then deciphers the conventional encryption

$$enc(u, (B \| P_B \| C_B \| x_B))$$

using session key u to find the identifier, public key, and certificate of the alleged party B. A verifies certificate C_B, and if positive it then uses the verification function, V_B to verify B's signature BS. If positive it then accepts u as a shared secret key.

B.8. ElGamal key transfer

This [7] is an example of Key Transport Mechanism 1. An appropriate prime p and generator g of Z_p^* are selected and made public. B's private and public key agreement keys are, respectively, h_B and

$$p_B = g^{h_B} \bmod p$$

Key Token Construction (A1) A has obtained a key K (in the range $0<K<p$) and wants to transfer it securely to B. A randomly and secretly generates a random integer r, $1 < r < p\text{-}1$, and enciphers K as

$$BE = K \cdot (p_B)^r \bmod p$$

Then A constructs the key token

$$KT_{A1} = BE \| g^r \bmod p$$

and sends it to B.

Key Token Deconstruction (B1) B recovers the key K using its private key agreement key h_B, computing

$$K = BE \cdot (g^r)^{-h_B} \bmod p$$

B.9. ElGamal key transfer with originator's signature

This is an example of Key Transport Mechanism 2. An appropriate prime p and generator g of Z_p^* are selected and made public. B's private and public key agreement keys are, respectively, h_B and

$$p_B = g^{h_B} \bmod p$$

A's private and public signature transformations are respectively denoted S_A and V_A; (S_A, V_A) could denote any signature system, for example RSA signature and signature verification as defined in ISO/IEC 9796.

Key Encipherment (A1.1) A has obtained a key K and wants to transfer it securely to B. A randomly and secretly generates a random integer r, in $\{1, \ldots, p\text{-}2\}$ and enciphers the key data block $A \| K$ as

$$BE = (A \| K) \cdot (p_B)^r \bmod p$$

Note that K must be chosen in such a way that the value of $(A \| K)$ is less than the prime p.

Key Token Construction (A1.2) A forms the token data block, consisting of the recipient's distinguished identifier B, an optional time stamp or sequence number TVP, g^r and the enciphered block BE. Then A signs the token data block using its private signature transformation S_A and sends the resulting key token

$$KT_{A1} = S_A\,(B||TVP||g^r||BE)$$

to B.

Key Token Verification (B1.1) B uses the sender's public verification transformation V_A to verify the digital signature of the received key token KT_{A1}. Then B checks the receiver identification B and optionally the TVP.

Key Decipherment (B1.2) B deciphers the block BE using its private key agreement key h_B, computing

$$A||K = BE \cdot (g^r)^{-h_B} \bmod p$$

Then B checks the sender identification A. If all checks are successful, B accepts the key K.

B.10. RSA key transfer

This is an example of Key Transport Mechanism 1. B's asymmetric encipherment system (E_B, D_B) consists of an RSA modulus $n = pq$, with public exponent e and private exponent d such that $ed = 1 \bmod (p-1)(q-1)$. A is assumed to have an authentic copy of B's encipherment parameters (e,n).

Key Token Construction (A1) A obtains a key K to transfer to B. Assume *Text1*, *Text2* and the optional *TVP* are all null (i.e. are omitted). Assume further that the data has been formatted adequately for RSA processing (e.g. by including some redundancy). A creates and sends to B the data block

$$KT_{A1} = E_B\,(A||K) = (A||K)^e \bmod n$$

Key Token Deconstruction (B1) B receives this and computes

$$(KT_{A1})^d \bmod n = (A||K).$$

The receiver B can distinguish this message from a random message by checking some redundancy condition in the message content $A||K$.

Assuming also that the identity A within this recovered message has some verifiable redundancy or expected format, B checks that the recovered identifier A' has the expected form, and accepts the message only if this check succeeds.

Annex C
(informative)

Examples of elliptic curve based key establishment mechanisms

The purpose of this annex is to show how key establishment mechanisms described in this part of ISO/IEC 11770 can be realized in terms of elliptic curves. The selection of the protocols presented follows widely Annex B.

Mathematical background on elliptic curves:

An elliptic curve E is a non-singular cubic curve defined over some field K. An elliptic curve can be described as the set of solutions (x, y) (x, y $\in K$) of an equation

$$Y^2 = X^3 + aX + b$$

together with an extra point q, the point at infinity.

Elliptic curves are endowed with a binary operation

$\circ$: E □ $E \rightarrow E$, adjoining to each pair (P_1,P_2) of points on E a third point $P_1 \circ P_2$. With respect to this operation E is a *abelian group* with neutral element q.

Let P be some point on an elliptic curve E generating a cyclic group $<P>$ of finite cardinality q with respect to the group operation "$\circ$". Then, each element of $<P>$ is some "power" $P^{[k]}$ of P, where $P^{[k]}$ is just an abbreviation for $(P \circ P \circ \ldots \circ P)$, k times.

The *discrete exponentiation $F(,P)$ on $<P>$* is defined by

$$F(k,P) = P^{[k]} \text{, for } k \in \{1, \ldots , q\text{-}1\}.$$

Note, that for arbitrary h, $k \in \{1, \ldots , q\text{-}1\}$ the equation

$$(P^{[h]})^{[k]} = P^{[h]\cdot[k]} = (P^{[k]})^{[h]}$$

holds, as the group $<P>$ generated by P is abelian.

On the other hand, given some arbitrary point $Q \in <P>$, the uniquely determined integer x $\in \{1, \ldots , q\text{-}1\}$with $Q = P^{[x]}$ is referred to as the *discrete logarithm* of Q to the base P.

The cryptographic importance of elliptic curves stems on the presumed difficulty to determine discrete logarithms on elliptic curves defined over finite fields, which - at current knowledge - is much harder than factorization of integers or calculating discrete logarithms in GF(p). This makes it possible to run an elliptic curve based public key system with much smaller parameters than in the case of the more familiar public key systems.

Notation:

The terminology introduced in the previous paragraph may hold for the sequel of this appendix.

In addition, let us fix the following notation:

K is a finite field consisting of exactly p^n elements, where p is a prime greater than 3 and n is a positive integer.

E is an elliptic curve over K and P is a point on E generating a cyclic group $<P>$ of cardinality q. We assume that q is a prime and set $H = \{1, \ldots , q\text{-}1\}$.

Each entity X have a private key h_X in H, which is only known by X, and a public key $P_X = G^{[hX]}$ known by all other entities.

Note, that the *private keys* are just *ordinary integers*, whereas the *public keys* are *points* on a *curve*. This is in contrast to public key systems based on discrete logarithms modulo a prime, where both keys are objects of the same type. This difference between the two types of keys in the case of elliptic curves is the reason why one has to introduce an additional function mapping the points of $<P>$ to integers in H, if one wants to transcript the protocols of Annex B to elliptic curves.

So, let π: $<P> \rightarrow H$ be a function such that the concatenation of π and $F(\cdot,P)$, given by

$$k \rightarrow P^{[k]} \rightarrow \pi(P^{[k]})$$

is one-way.

NOTES:

1 - The crucial parameter for the security of elliptic curve based public key systems is the size of the prime q. The integer q must be large enough so that $F(\cdot,P)$ can be considered to be a one-way function. With the currently available algorithms in mind, $F(\cdot,P)$ is one-way, if q is of size $q > 2^{160}$.

2 - Unlike the situation in $GF(p)^*$ based discrete logarithm systems (like DSA), it is possible to choose the parameters q and p^n of roughly the same size.

3 - There are some other conditions concerning the primes p and q (e.g., $p \neq q$) and the curve parameters a and b that must hold in order to make the computation of discrete logarithms on elliptic curves infeasible.

4 - There are many possibilities to define π. One simple method is to project the points of $<P>$ to their x-coordinate and to "read" this field element as an integer mod q.

C.1. Non-interactive key agreement of Diffie-Hellman type

This is an example of Key Agreement Mechanism 1.

Key Construction (A1) A computes, using its own private key agreement key h_A and B's public key agreement key P_B, the shared key as

$$K_{AB} = (P_B)^{[hA]}.$$

Key Construction (B1) B computes, using its own private key agreement key h_B and A's public key agreement key P_A, the shared key as

$$K_{AB} = (P_A)^{[hB]} .$$

C.2. Key agreement of ElGamal type

This is an example of Key Agreement Mechanism 2.

Key Token Construction (A1) A randomly and secretly generates r in H, computes $(P_B)^{[r]}$, constructs the key token

$$KT_{A1} = (P)^{[r]}$$

and sends it to B.

Key Construction (A2) A computes the shared key

$$K_{AB} = (P_B)^{[r]} = P^{[hB \cdot r]}.$$

Key Construction (B1) B computes with its own private key the shared key from KT_{A1} as follows:

$$K_{AB} = (KT_{A1})^{[hB]} = (P^{[r]})^{[hB]} = P^{[r \cdot hB]}.$$

C.3. Key agreement following Nyberg-Rueppel

This is an example of Key Agreement Mechanism 3. The protocol is not a 1-1-transcript of protocol B.3; but follows the essential ideas of B.3.

The signature system and the key agreement system are chosen in such a way that the signature system is determined by the keys (h_X, P_X).

To prevent from replay of old key tokens this example makes use of a time-stamp or a serial number TVP, and of a cryptographic hash function $hash$, which maps strings of bits of arbitrary length to random integers into H, for example.

Key Construction (A1.1) A randomly and secretly generates r in H and computes

$$R = P^{[r]}.$$

Further A computes the shared secret key as

$$K_{AB} = (P_B)^{[r]}.$$

Using the shared secret key K_{AB} A computes a cryptographic check value on the point R, the sender's distinguished identifier A and a sequence number or time-stamp TVP:

$$e = hash(R||K_{AB}||A||TVP)$$

Key Token Signature (A1.2) A computes the signature

$$y = (r - h_A \cdot e) \bmod q,$$

forms the key token

$$KT_{A1} = (R||A||TVP||y)$$

and sends it to B.

Key Construction (B1.1) *B* computes the shared secret key, using its private key agreement key h_B,

$$K_{AB} = R^{[h_B]}.$$

Using the shared secret key K_{AB} entity *B* computes the cryptographic check value on the sender's distinguished identifier *A* and the *TVP* and computes

$$e = hash(R||K_{AB}||A||TVP).$$

Signature Verification (B1.2) *B* checks the validity of *TVP* and verifies, using the sender's public key P_A, the equality

$$R = P^{[y]} \circ (P_A)^{[e]}.$$

C.4. Key agreement of Diffie-Hellman type

This is an example of Key Agreement Mechanism 4.

Key Token Construction (A1) *A* randomly and secretly generates r_A in *H*, computes $P^{[rA]}$, constructs the key token

$$KT_{A1} = P^{[rA]}$$

and sends it to *B*.

Key Token Construction (B1) *B* randomly and secretly generates r_B in *H*, computes $P^{[rB]}$, constructs the key token

$$KT_{B1} = P^{[r_B]}$$

and sends it to *A*.

Key Construction (A2) *A* computes the shared key

$$K_{AB} = (P^{[rB]})^{[rA]} = P^{[rB]\cdot[rA]}.$$

Key Construction (B2) *B* computes the shared key

$$K_{AB} = (P^{[rA]})^{[rB]} = P^{[rA]\cdot[rB]}.$$

C.5. Key agreement of Matsumoto-Takashima-Imai type A(0)

This is an example of Key Agreement Mechanism 5.

Key Token Construction (A1) *A* randomly and secretly generates r_A in *H*, computes the key token

$$KT_{A1} = P^{[rA]}$$

and sends it to *B*.

Key Token Construction (B1) *B* randomly and secretly generates r_B in *H*, computes the key token

$$KT_{B1} = P^{[rB]}$$

and sends it to *A*.

Key Construction (B2) *B* computes the shared key as

$$K_{AB} = w(KT_{A1}{}^{[hB]}, P_A{}^{[rB]})$$

where *w* is a one-way function.

Key Construction (A2) *A* computes the shared key as

$$K_{AB} = w(KT_{B1}{}^{[hA]}, P_B{}^{[rA]}).$$

C.6. Key transfer of ElGamal type

This is an example of Key Transport Mechanism 1.

Key Token Construction (A1) *A* has obtained a key *K* ∈H and wants to transfer it securely to *B*.

A randomly and secretly generates an integer $r \in H$, computes the curve point $P^{[r]}$and enciphers *K* as

$$BE = (K \cdot \pi((P_B)^{[r]})) \bmod q.$$

Then *A* constructs the key token

$$KT_{A1} = BE \,||\, (P^{[r]})$$

and sends it to *B*.

Key Token Deconstruction (B1) To recover the key *K*, entity *B* determines from $(P^{[r]})$, using its private key agreement key h_B, the curve point $(P_B)^{[r]} = (\mathrm{P}^{[r]})^{[h_B]}$ and in the next step the projection $\pi((P_B)^{[r]})$.

Finally, *B* obtains the key *K* by computing

$$K = (\mathrm{BE}) \cdot (\pi((P^{[r]})^{[h_B]}))^{-1} \bmod q.$$

C.7. Key transfer of ElGamal type with originator's signature

This is an example of Key Transport Mechanism 2. B's private and public key agreement keys are, respectively, h_B and

$$P_B = (P)^{[h_B]}\,.$$

A's private and public signature transformations are respectively denoted S_A and V_A; (S_A, V_A) could denote any signature system, for example one of the signature systems defined in ISO/IEC 9796.

Key Encipherment (A1.1) A has obtained a key K and wants to transfer it securely to B. A randomly and secretly generates an integer $r \in H$, the curve points $P^{[r]}$, $(P_B)^{[r]}$ and enciphers the key data block $A||K$ as

$$BE = (A||K)\cdot(\pi\,((P_B)^{[r]}))\bmod q.$$

Note that K must be chosen in such a way that the value of $(A||K)$ is less than the prime q.

Key Token Construction (A1.2) A forms the token data block, consisting of the recipient's distinguished identifier B, an optional time stamp or sequence number TVP and the enciphered block BE. Then A signs the token data block using its private signature transformation S_A and sends the resulting key token

$$\mathrm{KT}_{\mathrm{A1}} = (B||TVP||P^{[r]}||BE)$$

and its signature

$$\mathrm{S_A}(B||TVP||P^{[r]}||BE)$$

to B.

Key Token Verification (B1.1) B uses thc sender's public verification transformation V_A to verify the digital signature of the received key token KT_{A1}. Then B checks the rcceiver identification B and optionally thc TVP.

Key Decipherment (B1.2) B deciphers the block BE using its private key agreement key h_B, computing

$$(A||K) = (BE)\cdot(\pi\,((P^{[r]})^{[hB]}))^{-1}\bmod q$$

Then B checks the sender identification A. If all checks are successful, B accepts the key K.

Annex D
(informative)

Bibliography

[1] ANSI X9.30 199x, "Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA)".

[2] ANSI X9.30 199x, "Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 3: Certificate Management for DSA".

[3] ANSI X9.31 199x, "Public key cryptography using reversible algorithms for the financial services industry - Part 4: Management of symmetric algorithm keys using RSA".

[4] Beller M.J., Yacobi Y., "Fully-fledged two-way public authentication and key agreement for low-cost terminals", Electronic Letters, Vol. 29, no. 11 (27 May 93), pp 999-1001.

[5] RIPE, "Integrity Primitives for Secure Information Systems"- Final Report of RACE Integrity Primitives Evaluation (RIPE-RACE 1040), LNCS 1007, A. Bosselaers, B. Preneel, Eds., Springer-Verlag, 1995.

[6] Diffie W., Hellman M.E., "New Directions in Cryptography", IEEE Trans. on Inform. Theory, vol. IT-22, pp. 644-654, Nov. 1976.

[7] ElGamal, T., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. on Inform. Theory, vol. IT-31, pp. 469-472, July 1985.

[8] Girault M., Paillès J.C., "An identity-based scheme providing zero-knowledge authentication and authenticated key exchange", Proceedings of ESORICS 90, pp. 173-184.

[9] ISO 8732:1988, Banking - Key Management (Wholesale).

[10] ISO/IEC 9594-8: 1990, (CCITT X.509), "'Information technology - Open Systems Interconnection - The Directory - Authentication framework".

[11] ISO/IEC 9796: 1991, "'Information technology - Security techniques - Digital signature scheme giving message recovery".

[12] ISO/IEC 10118-2: 1994, "Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher algorithm".

[13] ISO/IEC 10118-3: 1998, "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash functions".

[14] ISO/IEC 10118-4: 1998, "Information technology - Security techniques - Hash-functions - Part 4: Mechanisms using modular arithmetic".

[15] ISO 11166-1: 1994, "Banking - Key Management by means of asymmetric algorithms - Part 1: Principles, Procedures and Formats".

[16] Matsumoto T., TakashimaY., Imai H., "On Seeking Smart Public-Key-Distribution Systems", Trans. of the IECE of Japan, vol.E69 no.2, Feb.1986 pp.99-106.

[17] Menezes, A., "Elliptic Curve Public Key Crytosystems", Kluwer Academic Publishers, 1993.

[18] Nyberg K., Rueppel R.A., "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem", Proceedings of Eurocrypt'94, Springer-Verlag, 1994.

[19] Okamoto E., "Proposal for identity-based key distribution system", Electronic Letters, Vol. 22, n°24, 20 Nov. 86, pp. 1283-4.

[20] Tanaka K., Okamoto E., "Key distribution system for mail systems using ID-related information directory", Computers & Security, Vol.10, 1991, pp. 25-33.

Annex E
(informative)

Patent Information

During the preparation of this International Standard [part 3 of ISO/IEC 11770], information was gathered concerning relevant patents upon which application of this International Standard might depend. Relevant patents were identified as shown in the table below. However, ISO/IEC cannot give authoritative or comprehensive information about the validity or scope of patents.

The identified patent-holders have stated that licenses will be granted in appropriate terms to enable application of this International Standard, provided that those who seek licenses agree to reciprocate.

Further information is available from the identified patent-holders.

Area	Inventors	Patent #	Issue date	Contact address
Diffie-Hellman key agreement	Hellman-Diffie-Merkle	US 4,200,770	1980-04-29	
RSA system	Rivest-Shamir-Adleman	US 4,405,829	1983-09-20	RSA Data Security, Inc. Director of Licensing 2955 Campus Drive, Suite 400 San Mateo, CA 94403-2507, USA
ID based DH key agreement	Eiji Okamoto	JP 1871933 US 4876716 EP 0257585 CA 1279709	1994-09-26 1989-10-24 1992-11-25 1991-01-01	NEC Corporation Intellectual Property Division 7-1, Shiba 5-Chome, Minato-Ku Tokyo 108-8001, Japan
Goss key agreement	Goss	US 4,956,863	1990-09-11	Jones Futurex™ Inc. Chief Operating Officer 3715 Atherton Road Rocklin, CA 95765, USA
ID based DH key agreement	Eiji Okamoto Kazue Tanaka	JP 1871933 US 4876716 EP 0257585 CA 1279709 AS 618229	1998-01-09 1991-07-02 1997-08-06 1995-01-03 1992-05-04	NEC Corporation Intellectual Property Division 7-1, Shiba 5-Chome, Minato-Ku Tokyo 108-8001, Japan
Nyberg-Rueppel key agreement	Nyberg-Rueppel	US 5,600,725 EP 0,639,907	1997-02-04 pending	Certicom Corp. 200 Matheson Blvd. West Missisauga, Ontario, Canada L5R 3L7 R^3 Security Engineering AG CH-8301 Glattzentrum, Switzerland

ICS 35.040

Price based on 35 pages

38

Office Action Summary	**Application No.** 09/710,916	**Applicant(s)** SLUIJTER ET AL.	
	Examiner ABUL K. AZAD	**Art Unit** 2654	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2003* .

2a)☒ This action is **FINAL.** 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *10-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☒ The proposed drawing correction filed on *01 July 2003* is: a)☒ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) □ Interview Summary (PTO-413) Paper No(s). _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: .

DETAILED ACTION

Response to Amendment

1. This action is in response to the communication filed on July 1, 2003.

2. Claims 10-30 are pending in this action. Claims 1-9 have been canceled. Claims 10-30 have been newly added.

Claim Rejections - 35 USC § 102

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

3. Claims 10, 12, 17, 18, 26 and 28 are rejected under 35 U.S.C. 102(a) as being anticipated by Kondo et al. (US 5,867,815).

As per claim 10, Kondo teaches, "a transmission system", comprising:

"a transmitter including a splitter for splitting up a transmission signal into a low frequency signal within a low frequency range and a high frequency signal within a high frequency range, the low frequency range being lower tan the high frequency range" (Fig. 1, element 1 is an encoder apparatus/transmitter, element 11 is splitter),

"wherein said splitter applies a low-pass filter to the transmission signal to generate the low frequency signal" (Fig. 1, element 11, is a low-pas filter),

"wherein said splitter applies a delay to the transmission signal to generate a delayed transmission signal, and wherein said splitter determines a difference between the low frequency signal and the delayed transmission signal to generate the high frequency signal" (Fig. 1, element 14, more details described at Fig. 3 and 4), "a first coder for deriving a first coded signal within the first frequency range from the low frequency signal" (Fig. 1, element 16 speech band coder is first encoder), and

"a second coder for deriving a second coded signal within the high frequency range from the high frequency signal" (Fig. 1, element 17 noise encoder is a second coder);

"a receiver in electrical communication with said transmitter to receive the first coded signal and the second coded signal" (Fig. 1, element 2 decoding apparatus is a receiver),

"said receiver including a first decoder for forming a first reconstructed signal within the first frequency range based on the first coded signal, and a second decoder for forming a second reconstructed signal within the second frequency range based on the second coded signal and a noise signal" (Fig. 1, elements 22 and 23 are speech decoder and noise decoder as first decoder and second decoder).

As per claim 26, it is interpreted and thus rejected for the same reason set forth in the rejection of claim 10.

As per claims 12 and 28, Kondo teaches, "wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code" (col. 5, lines 21-40);

"wherein said second coder determines prediction coefficients based on the high frequency signal" (col. 5, lines 41-46); and

"wherein the second coded signal codes the amplification code and the prediction coefficients as components of the second coded signal" (col. 5, lines 21-46).

As per claim 17, Kondo teaches, "a combiner for combining the first reconstructed signal and the second reconstructed signal" (Fig. 1, element 26).

As per claim 18, Kondo teaches, "wherein said receiver applies a delay to one of the first reconstructed signal and the second reconstructed signal prior to said combiner combining the first reconstructed signal and the second reconstructed signal" (col. 6, lines 5-6, here discrimination apparatus is according to Fig. 3 and 4, which includes a delay).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 11, 13, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kondo et al. (US 5,867,815) as applied to claims 10 and 26 above, and further in view of Abe et al. (US 5,581,652).

As per claims 11 ands 13, Kondo does not explicitly teach, "wherein said first coder sequentially applies a down-sampler and a narrowband coder to generate the first coded signal";

"wherein the first decoder sequentially applies a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate the first reconstructed signal".

However, Abe teaches, "wherein said first coder sequentially applies a down-sampler and a narrowband coder to generate the first coded signal" (Fig. 2, element 200 and Fig. 4, element 302 as narrow band coder);

"wherein the first decoder sequentially applies a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate the first reconstructed signal" (Fig. 8, elements 501, 406, 503 and 505).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a first encoder and a decoder as described by Abe in the invention of Kondo so that a narrow band coded signal can be easily transmitted through a conventional telephone line and a wideband signal can be reconstructed at the decoding end have a perceptual quality.

6. Claims 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kondo et al. (US 5,867,815) in view of well-known art.

As per claim 14, Kondo teaches, "wherein, based on the second coded signal, the second decoder sequentially applies a LPC synthesis filter and an amplifier to the noise signal to generate the second reconstructed signal (col. 5, lines 21-56).

As per claim 14, Kondo does not explicitly teach a high-pass filter. Official Notice is taken to a well-known high-pass filter used at the decoder side to produce unvoiced signal from a random noise generator. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a high-pass filter so as to pass only higher ban speech signal to produce unvoiced part of speech of perceptual quality.

As per claim 15, Kondo teaches, "wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code" (col. 5, lines 21-40) ;

"wherein said second coder codes the amplification code as one component of the second coded signal" (col. 5, lines 41-46); and

"wherein said second decoder uses the amplification code to set said amplifier" (col. 5, lines 21-40).

As per claim 16, Kondo teaches, "wherein said second coder determines prediction coefficients based on the high frequency signal; wherein said second coder codes the prediction coefficients as one component of the second coded signal, and wherein said second decoder uses the prediction coefficients to control said LPC synthesis filter" (col. 5, lines 46-56).

7. Claims 19-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kondo et al. (US 5,867,815) in view of Abe et al. (US 5,581,652) further in view of well-known art.

As per claim 19, Kondo teaches, "a transmission system", comprising:

a transmitter including a splitter for splitting up a transmission signal into a low frequency signal within a low frequency range and a high frequency signal within a high frequency range, the low frequency range being lower than the high frequency range" (Fig. 1, element 1 is an encoder apparatus/transmitter, element 11 is splitter),

"a first coder for deriving a first coded signal within the first frequency range from the low frequency signal and a second coder for deriving a second coded signal within the high frequency range from the high frequency signal" (Fig. 1, element 16 speech band coder is first encoder and Fig. 1, element 17 noise encoder is a second coder);

"a receiver in electrical communication with said transmitter to receive the first coded signal and the second coded signal" (Fig. 1, element 2 decoding apparatus is a receiver).

As per claim 19, Kondo does not explicitly teach, "said receiver including a first decoder for sequentially applying a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate a first reconstructed signal within the first frequency range, and a second decoder". However, Abe teaches, "wherein the first decoder sequentially applies a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate the first reconstructed signal" (Fig. 8, elements 501, 406, 503 and 505).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a first encoder and a decoder as described by Abe in the invention of Kondo so that a narrow band coded signal can be easily transmitted through a conventional telephone line and a wideband signal can be reconstructed at the decoding end have a perceptual quality.

Kondo teaches, "wherein, based on the second coded signal, said second decoder sequentially applies a LPC synthesis filter and an amplifier to a noise signal to generate the second reconstructed signal" (col. 5, lines 21-56).

Kondo does not explicitly teach a high-pass filter. Official Notice is taken to a well-known high-pass filter used at the decoder side to produce unvoiced signal from a random noise generator. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a high-pass filter so as to pass only higher ban speech signal to produce unvoiced part of speech of perceptual quality.

As per claim 29, it is interpreted and thus rejected for the same reasons set forth in the rejection of claim 19.

As per claim 20, Kondo does not explicitly teach, "wherein said first coder sequentially applies a down-sampler and a narrow-band coder to generate the first coded signal". However, Abe teaches, "wherein said first coder sequentially applies a down-sampler and a narrowband coder to generate the first coded signal" (Fig. 2, element 200 and Fig. 4, element 302 as narrow band coder);

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a first encoder and a decoder as described by Abe in the invention of Kondo so that a narrow band coded signal can be easily transmitted through a conventional telephone line and a wideband signal can be reconstructed at the decoding end have a perceptual quality.

As per claims 21-25 and 30, they are interpreted and thus rejected for the same reasons set forth in the rejection of claims 14-18.

Response to Arguments

8. Applicant's arguments with respect to claims 1-9 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Abul K. Azad** whose telephone number is **(703) 305-3838.**

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Richemond Dorvil**, can be reached at **(703) 305-9645.**

Any response to this action should be mailed to:

Commissioner for Patents

Washington, D.C. 20231

Or faxed to:

(703) 872-9314

(For informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Sixth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application should be directed to the Technology Center's Customer Service Office whose telephone number is **(703) 306-0377.**

Abul K. Azad
September 21, 2003

Richemond Dorvil
Primary Examiner

39

Certificate of Facsimile
I hereby certify that this correspondence is being transmitted by facsimile to (703) 872-9315 to the U.S. Patent and Trademark Office November 20, 2003
(Date of Deposit)

DARRIN WESLEY HARRIS (40,636)
Name of applicant, assignee or registered representative

Signature

November 20, 2003
Date of Signature

PATENT
Case No. PHN 17,764
(7790/257)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:	)	
	)	
ROBERT J. SLUIJTER ET AL.	)	
	)	Examiner: AZAD, ABUL K.
Serial No.: 09/710,916	)	
	)	Group Art Unit: 2654
Filed: NOVEMBER 13, 2000	)	
	)	
For: WIDEBAND AUDIO TRANSMISSION SYSTEM	)	

RESPONSE TO A FINAL OFFICE ACTION DATED SEPTEMBER 25, 2003

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to a Final Office Action dated September 25, 2003, please amend the above-identified application as follows:

CLAIM AMENDMENTS

Claims 10-30 are currently pending in the application.

Please amend claims 10, 12-14, 17, 19, 21, 28 and 29 for non-statutory purposes as shown below.

The following listing of claims 1-30 will replace all prior versions, and listings, of claims in the application:

1.-9. (Cancelled)

10. (Currently Amended) A transmission system, comprising:

a transmitter including

a splitter for splitting up a transmission signal into a low frequency signal within a low frequency range and a high frequency signal within a high frequency range, the low frequency range being lower than the high frequency range,

wherein said splitter applies a low-pass filter to the transmission signal to generate the low frequency signal,

wherein said splitter applies a delay to the transmission signal to generate a delayed transmission signal, and

wherein said splitter determines a difference between the low frequency signal and the delayed transmission signal to generate the high frequency signal,

a first coder for deriving a first coded signal within the first frequency range from the low frequency signal, and

a second coder for deriving a second coded signal within the high frequency range from the high frequency signal; and

a receiver in electrical communication with said transmitter to receive the first coded signal and the second coded signal, said receiver including

a first decoder for forming a first reconstructed signal within the first frequency range based on the first coded signal, and

a second decoder for forming a second reconstructed signal within the second frequency range based on the second coded signal and a noise signal.

11. (Previously Presented) The transmission system of claim 10,

wherein said first coder sequentially applies a down-sampler and a narrow-band coder to generate the first coded signal.

12. (Currently Amended) The transmission system of claim 10,

wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code;

wherein said second coder determines prediction coefficients based on the high frequency signal; and

wherein ~~the~~ said second ~~coded signal~~ coder codes the amplification code and the prediction coefficients as components of the second coded signal.

13. (Currently Amended) The transmission system of claim ~~11~~ 10,

wherein ~~the~~ said first decoder sequentially applies a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate the first reconstructed signal.

14. (Currently Amended) The transmission system of claim ~~11~~ 10,

wherein, based on the second coded signal, ~~the~~ said second decoder sequentially applies a high-pass filter, a LPC synthesis filter and an amplifier to the noise signal to generate the second reconstructed signal.

15. (Previously Presented) The transmission system of claim 14,

wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code;

wherein said second coder codes the amplification code as one component of the second coded signal; and

wherein said second decoder uses the amplification code to set said amplifier.

16. (Previously Presented) The transmission system of claim 14,

wherein said second coder determines prediction coefficients based on the high frequency signal;

wherein said second coder codes the prediction coefficients as one component of the second coded signal, and

wherein said second decoder uses the prediction coefficients to control said LPC synthesis filter.

17. (Currently Amended) The transmission system of claim ~~11~~ 10, further comprising:

a combiner for combining the first reconstructed signal and the second reconstructed signal.

18. (Previously Presented) The transmission system of claim 17,

wherein said receiver applies a delay to one of the first reconstructed signal and the second reconstructed signal prior to said combiner combining the first reconstructed signal and the second reconstructed signal.

19. (Currently Amended) A transmission system, comprising:

a transmitter including

a splitter for splitting up a transmission signal into a low frequency signal within a low frequency range and a high frequency signal within a high frequency range, the low frequency range being lower than the high frequency range,

a first coder for deriving a first coded signal within the first frequency range from the low frequency signal, and

a second coder for deriving a second coded signal within the high frequency range from the high frequency signal; and

a receiver in electrical communication with said transmitter to receive the first coded signal and the second coded signal, said receiver including

a first decoder for sequentially applying a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate a first reconstructed signal within the first frequency range, and a second decoder, wherein, based on the second coded signal, said second decoder sequentially applies a high-pass filter, a LPC synthesis filter and an amplifier to a noise signal to generate the second reconstructed signal.

20. (Previously Presented) The transmission system of claim 19,

wherein said first coder sequentially applies a down-sampler and a narrow-band coder to generate the first coded signal.

21. (Currently Amended) The transmission system of claim 19,

wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code;

wherein said second coder determines prediction coefficients based on the high frequency signal; and

wherein ~~the~~ said second ~~coded signal~~ coder codes the amplification code and the prediction coefficients as components of the second coded signal.

22. (Previously Presented) The transmission system of claim 19,

wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code;

wherein said second coder codes the amplification code as one component of the second coded signal; and

wherein said second decoder uses the amplification code to set said amplifier.

23. (Previously Presented) The transmission system of claim 19,

wherein said second coder determines prediction coefficients based on the high frequency signal;

wherein said second coder codes the prediction coefficients as one component of the second coded signal, and

wherein said second decoder uses the prediction coefficients to control said LPC synthesis filter.

24. (Previously Presented) The transmission system of claim 19, further comprising:

a combiner for combining the first reconstructed signal and the second reconstructed signal.

25. (Previously Presented) The transmission system of claim 24,

wherein said receiver applies a delay to one of the first reconstructed signal and the second reconstructed signal prior to said combiner combining the first reconstructed signal and the second reconstructed signal.

26. (Previously Presented) A transmitter, comprising:

a splitter for splitting up a transmission signal into a low frequency signal within a low frequency range and a high frequency signal within a high frequency range, the low frequency range being lower than the high frequency range,

wherein said splitter applies a low-pass filter to the transmission signal to generate the low frequency signal,

wherein said splitter applies a delay to the transmission signal to generate a delayed transmission signal, and

wherein said splitter determines a difference between the low frequency signal and the delayed transmission signal to generate the high frequency signal;

a first coder for deriving a first coded signal within the first frequency range from the low frequency signal; and

a second coder for deriving a second coded signal within the high frequency range from the high frequency signal.

27. (Previously Presented) The transmitter of claim 26,

wherein said first coder sequentially applies a down-sampler and a narrow-band coder to generate the first coded signal.

28. (Currently Amended) The transmission system of claim 26,

wherein said second coder measures a signal strength of the high frequency signal to generate an amplification code;

wherein said second coder determines prediction coefficients based on the high frequency signal; and

wherein ~~the~~ said second ~~coded signal~~ coder the amplification code and the prediction coefficients as components of the second coded signal.

29. (Currently Amended) A receiver, comprising:

a first decoder receiving a first coded signal with a low frequency range, said first decoder for sequentially applying a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate a first reconstructed signal within the low frequency range;

a second decoder receiving a second coded signal within a high frequency range that is higher the low frequency range,

wherein, based on the second coded signal, said second decoder sequentially applies a high-pass filter, a LPC synthesis filter and an amplifier to a noise signal to generate a second reconstructed signal within the high frequency range; and

a combiner for combining the first reconstructed signal and the second reconstructed signal.

30. (Previously Presented) The receiver of claim 29,

wherein said receiver applies a delay to one of the first reconstructed signal and the second reconstructed signal prior to said combiner combining the first reconstructed signal and the second reconstructed signal.

REMARKS

In the Final Office Action, Examiner Azad rejected pending claims 10-30 on various grounds. The Applicant responds to each rejection as subsequently recited herein, and respectfully requests reconsideration and further examination of the present application under 37 CFR § 1.116:

A. Examiner Azad rejected pending claims 10, 12, 17, 18, 26 and 28 under 35 U.S.C. §102(a) as being anticipated by U.S. Patent No. 5,867,815 to *Kondo* et al.

The Applicant has thoroughly considered Examiner Azad's remarks concerning the patentability of claims 10, 12, 17, 18, 26 and 28 over *Kondo*. The Applicant has also thoroughly read *Kondo*. To warrant this 35 U.S.C. §102(a) rejection of claims 10, 12, 17, 18, 26 and 28, *Kondo* must show each and every limitation of independent claims 10 and 26 in as complete detail as in contained in independent claims 10 and 26. See, MPEP §2131. The Applicant respectfully traverses this §102(a) rejection of claims 10, 12, 17, 18, 26 and 28, because *Kondo* fails to disclose and teaches away "wherein said splitter applies a delay to the transmission signal to generate a delayed transmission signal", and "wherein said splitter determines a difference between the low frequency signal and the delayed transmission signal to generate the high frequency signal" as recited in independent claims 10 and 26.

Specifically, as illustrated in FIG. 1, *Kondo* discloses splitter employing a low pass filter 11 for generating the low frequency signal ("voice band") form the transmission input signal, and a high pass filter 12 for generating the high frequency signal ("nonvoice band and background noise") from the transmission input signal. See, *Kondo* at column 2, line 56 to column 3, line 9.

The splitter as taught by *Kondo* clearly does not employ the nonvoice band detector 14, which is used instead for controlling a switch 15 whereby the high frequency signal as generated by the high pass filter 12 is applied to an adder 13 when detector 14 detected a nonvoice band within the high frequency signal and whereby the high frequency signal as generated by the high pass filter 12 is applied to a noise encoder 17 when detector 14 fails to detect a nonvoice band within the high frequency signal. See, *Kondo* at column 3, lines 10-66.

Kondo unequivocally fails to teach or suggest the aforementioned limitations of independent claims 10 and 16. Withdrawal of the rejection of independent claims 10 and 26 under §102(a) as being anticipated by *Kondo* is therefore respectfully requested.

Claims 12, 17 and 18 depend from independent claim 10. Therefore, dependent claims 12, 17 and 18 include all of the elements and limitations of independent claim 10. It is therefore respectfully submitted by the Applicant that dependent claims 12, 17 and 18 are allowable over *Kondo* for at least the same reason as set forth herein with respect to independent claim 10 being allowable over *Kondo*. Withdrawal of the rejection of dependent claims 12, 17 and 18 under 35 U.S.C. §102(a) being anticipated by *Kondo* is therefore respectfully requested.

Claim 28 depends from independent claim 26. Therefore, dependent claim 28 includes all of the elements and limitations of independent claim 26. It is therefore respectfully submitted by the Applicant that dependent claim 28 is allowable over *Kondo* for at least the same reason as set forth herein with respect to independent claim 26 being allowable over *Kondo*. Withdrawal of the rejection of dependent claim 28 under 35 U.S.C. §102(a) being anticipated by *Kondo* is therefore respectfully requested.

B. Examiner Azad rejected pending claims 11, 13 and 27 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,867,815 to *Kondo* et al. in view of U.S. Patent No. 5,581,652 to *Abe* et al.

Claims 11 and 13 depend from independent claim 10. Therefore, dependent claims 11 and 13 include all of the elements and limitations of independent claim 10. It is therefore respectfully submitted by the Applicant that dependent claims 11 and 13 are allowable over *Kondo* in view of *Abe* for at least the same reason as set forth herein with respect to independent claim 10 being allowable over *Kondo*. Withdrawal of the rejection of dependent claims 11 and 13 under 35 U.S.C. §103(a) being unpatentable over *Kondo* in view of *Abe* is therefore respectfully requested.

Claim 27 depends from independent claim 26. Therefore, dependent claim 27 includes all of the elements and limitations of independent claim 26. It is therefore respectfully submitted by the Applicant that dependent claim 27 is allowable over *Kondo* in view of *Abe* for at least the same reason as set forth herein with respect to independent claim 26 being allowable over *Kondo*. Withdrawal of the rejection of dependent claim 27 under 35 U.S.C. §103(a) being unpatentable over *Kondo* in view of *Abe* is therefore respectfully requested.

C. Examiner Azad rejected pending claims 14-16 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,867,815 to *Kondo* et al. in view of *well-known art*

Claims 14-16 depend from independent claim 10. Therefore, dependent claims 14-16 include all of the elements and limitations of independent claim 10. It is therefore respectfully submitted by the Applicant that dependent claims 14-16 are allowable over *Kondo* in view of *well-known art* for at least the same reason as set forth herein with respect to independent claim 10 being allowable over *Kondo*. Withdrawal of the rejection of dependent claims 14-16 under 35 U.S.C. §103(a) being unpatentable over *Kondo* in view of *well-known art* is therefore respectfully requested.

D. Examiner Azad rejected pending claims 19-25, 29 and 30 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,867,815 to *Kondo* et al. in view of U.S. Patent No. 5,581,652 to *Abe* et al and in further view of *well-known art*

The Applicant has thoroughly considered Examiner Azad's remarks concerning the patentability of claims 19-25, 29 and 30 over *Kondo* in view of *Abe* and in further view of *well-known art*. The Applicant has also thoroughly read *Kondo* and *Abe*. To warrant this 35 U.S.C. §103(a) rejection of claims 19-25, 29 and 30, all the claim limitations recited in independent claims 19 and 29 must be taught or suggested by the combination of *Kondo* and *Abe*. See, MPEP §2143. The Applicant respectfully traverses this §103(a) rejection of claims 19-25, 29 and 30, because *Kondo* and *Abe* in combination fails to disclose and teaches away the following limitations of independent claims 19 and 29:

1. "a first decoder for sequentially applying a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate a first reconstructed signal within the first frequency range", and "a second decoder, wherein, based on the second coded signal, said second decoder sequentially applies a high-pass filter, a LPC synthesis filter and an amplifier to a noise signal to generate the second reconstructed signal" as recited in independent claim 19; and

2. "a first decoder receiving a first coded signal with a low frequency range, said first decoder for sequentially applying a narrow-band decoder, an up-sampler and a low-pass filter to the first coded signal to generate a first reconstructed signal within the low frequency range", "a second decoder receiving a second coded signal within a high frequency range that is higher the low frequency range", and "wherein, based on the second coded signal, said second decoder sequentially applies a high-pass filter, a LPC synthesis filter and an amplifier to a noise signal to generate a second reconstructed signal within the high frequency range" as recited in independent claim 29.

As to the traversal, *Kondo* teaches coder with reference to FIG. 5, and a decoder with reference to FIG. 6 of *Kondo*. The coder of FIG. 5 is irrelevant to independent claims 19 and 29, because the scope of independent claims 19 and 29 encompass a decoder, not an coder.

The decoder of FIG. 6 is relevant, and clearly, as illustrated in FIG. 6, Kondo teaches a demultiplexing of a coded signal into a LPC parameter code, an IDX normalization coefficient, and a pitch parameter code. A LPC parameter decoder 72 is applied to a LPC parameter to generate a LPC parameter. A codebook decoder 73 is applied to the IDX normalization coefficient to generate a noise/nonvoice band. And, a pitch decoder 74 is applied to the pitch parameter code to generate a pitch parameter. See, *Kondo* at column 5, lines 47-67. *Kondo* unequivocally fails to teach or suggest a sequential application of a narrow-band decoder, an up-sampler, and a low-pass filter to a first coded signal, or a sequential application of a high-pass filter, a LPC synthesis filter, and an amplifier to a noise signal as a function of a second coded signal

As illustrated in FIG. 8, *Abe* discloses a narrowband speech signal that flows through a first path and a second path to an adder 505. The first path sequentially employs a LPC analyzer 401, a quantizer 402, a decoder 501, a LPC synthesizer 502, a low pass filter 503, and a power adjuster 504. The second path exclusively employs an up-sampler 406. *Abe* unequivocally fails to teach or suggest a sequential application of a narrow-band decoder, an up-sampler, and a low-pass filter to the narrowband speech signal.

Withdrawal of the rejection of independent claims 19 and 29 under §103(a) as being unpatentable over *Kondo* in view of *Abe* and in further view of *well-known art* is therefore respectfully requested.

Claims 20-25 depend from independent claim 19. Therefore, dependent claims 20-25 include all of the elements and limitations of independent claim 19. It is therefore respectfully submitted by the Applicant that dependent claims 20-25 are allowable over *Kondo* in view *Abe* and in further view of *well-known art* for at least the same reason as set forth herein with respect to independent claim 19 being allowable over *Kondo* in view *Abe* and in further view of *well-known art.* Withdrawal of the rejection of dependent claims 20-25 under 35 U.S.C. §103(a) being unpatentable over *Kondo* in view *Abe* and in further view of *well-known art* is therefore respectfully requested.

Claim 30 depends from independent claim 29. Therefore, dependent claim 30 includes all of the elements and limitations of independent claim 29. It is therefore respectfully submitted by the Applicant that dependent claim 30 is allowable over

Kondo in view *Abe* and in further view of *well-known art* for at least the same reason as set forth herein with respect to independent claim 29 being allowable over *Kondo* in view *Abe* and in further view of *well-known art*. Withdrawal of the rejection of dependent claim 30 under 35 U.S.C. §103(a) being unpatentable over *Kondo* in view *Abe* and in further view of *well-known art* is therefore respectfully requested.

SUMMARY

Examiner Azad's rejections of pending claims 10-30 have been obviated by the remarks herein supporting an allowance of pending claims 10-30 over the art of record. The Applicant respectfully submits that claims 10-30 as amended herein fully satisfy the requirements of 35 U.S.C. §§ 102, 103 and 112. In view of the foregoing, favorable consideration and early passage to issue of the present application is respectfully requested. If any points rcmain in issue that may best be resolved through a personal or telephonic interview, Examiner Azad is respectfully requested to contact the undersigned at the telephone number listed below.

Dated: **November 20, 2003**

Respectfully submitted,
Robert Johannes Sluijter et al.

PHILIPS INTELLECTUAL PROPERTY
& STANDARDS
P.O. Box 3001
Briarcliff, New York 10510
Phone: (914) 333-9612
Fax: (914) 332-0615

Jack D. Slobod
Registration No. 26,236
Attorney for Applicant

CARDINAL LAW GROUP
Suite 2000
1603 Orrington Avenue
Evanston, Illinois 60201
Phone: (847) 905-7111
Fax: (847) 905-7113

Darrin Wesley Harris
Registration No. 40,636
Attorney for Applicant

40

Notice of Allowability	Application No. 09/619,426	Applicant(s) Jan Van Ee
	Examiner Mansour M. Said	Art Unit 2673

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *05/13/2002* .

2. ☒ The allowed claim(s) is/are *9-14, and renumbered as 1-6* .

3. ☐ The drawings filed on ________ are accepted by the Examiner.

4. ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. ________ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   *Certified copies not received: ________ .

5. ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

   (a) ☐ The translation of the foreign language provisional application has been received.

6. ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

7. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

8. ☒ CORRECTED DRAWINGS must be submitted.

   (a) ☒ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) ☐ hereto or 2) ☒ to Paper No. *14* .

   (b) ☐ including changes required by the proposed drawing correction filed ________ , which has been approved by the examiner.

   (c) ☐ including changes required by the attached Examiner's Amendment/Comment or in the Office action of Paper No. ____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the top margin (not the back) of each sheet. The drawings should be filed as a separate paper with a transmittal letter addressed to the Official Draftsperson.

9. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1 ☐ Notice of References Cited (PTO-892)

2 ☐ Notice of Informal Patent Application (PTO-152)

3 ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)

4 ☐ Interview Summary (PTO-413), Paper No. ____ .

5 ☐ Information Disclosure Statement(s) (PTO-1449), Paper No(s). ________

6 ☒ Examiner's Amendment/Comment

7 ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

8 ☒ Examiner's Statement of Reasons for Allowance

9 ☐ Other

U. S. Patent and Trademark Office
PTO-37 (Rev. 04-01) **Notice of Allowability** Part of Paper No. 16

DETAILED ACTION

Terminal Disclaimer

1. The terminal disclaimer filed on 05/13/2002 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of Pat. # 6,211,856 has been reviewed and is accepted. The terminal disclaimer has been recorded.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Jeroen Heuvelman on May 29, 2002.

3. The application has been amended as follow:

IN THE CLAIMS

In claim 9 line 4, please cancel the phrase "in".

In claim 9 line 15, after "first scale" please add --, thereby facilitating a selection of a feature --.

C1

12

In claim 9 line 15, after ";" please enter -- and --.

In claim 14 line 5, please cancel the phrase "in"

c2 In claim 14 line 16, after "first scale" please add --, thereby facilitating a selection of a feature --.

In claim 14 line 16, after ";" please enter -- and --.

Allowable Subject Matter

4. The application having been allowed, formal drawings are required in response to this Office action.

5. The application having been allowed, formal drawings are required in response to this Office Action.

6. Claims 9-14 are allowed.

7. The following is an examiner's statement of reasons for allowance:

8. None of the prior art of the record either singularly or in combination teach or fairly suggest a handheld communication device comprising a wireless modem for receiving data; a display that has a substantially small size suitable for the handheld communication device; a data processing system connected to the modem and to the display for processing the received data and for rendering an image corresponding to the data received; a touch screen for enabling a user to interact with the device; wherein the system is operative to enable the user to select through a

13

touch location on the touch screen a portion of the image, when displayed at a first scale, for rendering the selected portion on the display at a second scale larger than the first scale, thereby facilitating a selection of a feature; and the selected portion when rendered at the first scale is a zoomed-in version of part of the image at the first scale substantially centered around the touch screen..

Cited Hirayama et al. (5,406,307) disclose an icon displayed on a display portion for indicating various functions with a point of the pen and drags the pen along the surface of the display portion to a display position and releases the point of the pen from the panel surface of the display portion, an enlarged processing display form is automatically displayed at a desired position of the display portion.

Cited Tanimoto et al. (5,969,706) teach an information retrieval apparatus includes a display section for displaying a first image; an enlargement section for continuously enlarging the first image displayed by the display section in response to an instruction of the user; and a determination section for determining that a magnification ratio of the first image enlarged by the enlargement section has reached a prescribed value.

However, both references fail to disclose the claimed limitations such as the system is operative to enable the user to select through a touch location on the touch screen a portion of the image, when displayed at a first scale, for rendering the selected portion on the display at a second scale larger than the first scale, thereby facilitating a selection of a feature; and the selected portion when rendered at the first scale is a zoomed-in version of part of the image at the first scale substantially centered around the touch screen.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Mansour M. Said** whose telephone number is **(703) 306-5411**.

The examiner can normally be reached on Monday through Thursday from 8:30 a.m. to 6:00 p.m. The examiner can also be reached on alternate Friday from 8:30 a.m. to 5:00 p.m. EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Shalwala Bipin**, can be reached at **(703) 305-4938**.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

or faxed to:

(703) 872-9314 (for Technology Center 2600 only)

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Sixth Floor (Receptionist)

10. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Technology Center 2600 Customer service Office whose telephone number is (703) 306-0377.

Patent Examiner

May 30, 2002

Mansour M. Said

BIPIN SHALWALA
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600